APPOINTMENT AFFIDAVITS

Senior Advisor to the Director
(Position to which Appointed)

01/20/2025
(Date Appointed)

Office of Personnel Management
(Department or Agency)

Office of the Director
(Bureau or Division)

Washington, DC, United States
(Place of Employment)

I, GREGORY JOHN HOGAN, do solemnly swear (or affirm) that--

A. OATH OF OFFICE

I will support and defend the Constitution of the United States against all enemies, foreign and domestic; that I will bear true faith and allegiance to the same; that I take this obligation freely, without any mental reservation or purpose of evasion; and that I will well and faithfully discharge the duties of the office on which I am about to enter. So help me God.

B. AFFIDAVIT AS TO STRIKING AGAINST THE FEDERAL GOVERNMENT

I am not participating in any strike against the Government of the United States or any agency thereof, and I will not so participate while an employee of the Government of the United States or any agency thereof.

C. AFFIDAVIT AS TO THE PURCHASE AND SALE OF OFFICE

I have not, nor has anyone acting in my behalf, given, transferred, promised or paid any consideration for or in expectation or hope of receiving assistance in securing this appointment.

[illegible]
(Signature of Appointee)

Subscribed and sworn (or affirmed) before me this 20 day of January, 2025

at Washington (City) DC (State)

[illegible]
(Signature of Officer)

(SEAL)

Commission expires ________
(If by a Notary Public, the date of his/her Commission should be shown)

Acting Director
(Title)

Note - If the appointee objects to the form of the oath on religious grounds, certain modifications may be permitted pursuant to the Religious Freedom Restoration Act. Please contact your agency's legal counsel for advice.

Standard Form 50
Rev. 7/91
U.S. Office of Personnel Management
FPM Supp. 296-33, Subch. 4

NOTIFICATION OF PERSONNEL ACTION

1. Name (Last, First, Middle) HOGAN, GREGORY JOHN	2. Social Security Number [redacted]	3. Date of Birth [redacted]	4. Effective Date 01/20/2025

FIRST ACTION

5-A. Code 146	5-B. Nature of Action SES NONCAREER APPT
5-C. Code V4L	5-D. Legal Authority 5 U.S.C. 3394(A).
5-E. Code AWM	5-F. Legal Authority OPM MEMO DTD 01-20-2025

SECOND ACTION

6-A. Code	6-B. Nature of Action
6-C. Code	6-D. Legal Authority
6-E. Code	6-F. Legal Authority

7. FROM: Position Title and Number

8. Pay Plan	9. Occ. Code	10. Grade or Level	11. Step or Rate	12. Total Salary	13. Pay Basis

12A. Basic Pay	12B. Locality Adj.	12C. Adj. Basic Pay	12D. Other Pay

14. Name and Location of Position's Organization

15. TO: Position Title and Number
SENIOR ADVISOR TO THE DIRECTOR FOR TECHNOLOGY AND DELIVERY
PD: 6A38081

16. Pay Plan	17. Occ. Code	18. Grade or Level	19. Step or Rate	20. Total Salary/Award	21. Pay Basis
ES	0301	00	00	$195,200.00	PA

20A. Basic Pay	20B. Locality Adj.	20C. Adj. Basic Pay	20D. Other Pay
$195,200.00	$0	$195,200.00	$0

22. Name and Location of Position's Organization
OPM
OFC OF THE DIRECTOR
WASHINGTON DC

EMPLOYEE DATA

23. Veterans Preference: 1 (1 - None; 2 - 5 Point; 3 - 10 Point/Disability; 4 - 10 Point/Compensable; 5 - 10 Point/Other; 6 - 10-Point/Compensable/30%)

24. Tenure: 0 (0 - None; 1 - Permanent; 2 - Conditional; 3 - Indefinite)

25. Agency Use: TG

26. Veterans Pref for RIF: YES [✓ NO]

27. FEGLI: B0 [redacted]

28. Annuitant Indicator: 9 NOT APPLICABLE

29. Pay Rate Determinant: 0

30. Retirement Plan: KF [redacted]

31. Service Comp. Date (Leave): 01/20/2025

32. Work Schedule: F FULL TIME

33. Part-Time Hours Per Biweekly Pay Period:

POSITION DATA

34. Position Occupied: 3 (1 - Competitive Service; 2 - Excepted Service; 3 - SES General; 4 - SES Career)

35. FLSA Category: E (E - Exempt; N - Nonexempt)

36. Appropriation Code: 41AA0

37. Bargaining Unit Status: 8888

38. Duty Station Code: 11-0010-001

39. Duty Station (City - County - State or Overseas Location): WASHINGTON DISTRICT OF COLUMBIA DC

40. AGENCY DATA	41.	42.	43.	44.
10001		0000	33.94	CRITICAL-SENSITIVE (CS)/HIGH R

45. Remarks

APPOINTMENT AFFIDAVIT EXECUTED 01-20-2025.

EMPLOYEE SUBJECT TO POST-EMPLOYMENT RESTRICTIONS UNDER 18 U.S.C. 207(C).

THE EMPLOYEE OCCUPIES A POSITION SUBJECT TO THE PAY FREEZE FOR CERTAIN SENIOR POLITICAL OFFICIALS. NOTWITHSTANDING OTHERWISE APPLICABLE PAY STATUTES AND REGULATIONS, PAY MAY BE SET AND ADJUSTED ONLY IN ACCORDANCE WITH APPLICABLE PROVISIONS OF THE PAY FREEZE STATUTE.

TENURE AS USED FOR 5 U.S.C. 3502 IS NOT APPLICABLE TO THE SENIOR EXECUTIVE SERVICE.

CREDITABLE MILITARY SERVICE:0000

PREVIOUS RETIREMENT COVERAGE: NEVER COVERED

EMPLOYEE IS AUTOMATICALLY COVERED UNDER FERS, FERS-RAE, OR FERS-FRAE.

UPON APPOINTMENT TO THIS POSITION, APPOINTEE RECEIVED AND SIGNED THE ETHICS PLEDGE. MEMBER RECEIVED FINANCIAL DISCLOSURE MEMORANDUM AND SF-278 WHICH IS TO BE COMPLETED AND RETURN WITHIN 30 DAYS OF APPOINTMENT. THIS IS A TEMPORARY APPOINTMENT WITH A NOT TO EXCEED DATE OF 2-19-2025.

46. Employing Department or Agency: OPM

47. Agency Code	48. Personnel Office ID	49. Approval Date
OM00	1000	01/27/2025

50. Signature/Authentication and Title of Approving Official
ELECTRONICALLY SIGNED BY:
CARMEN GARCIA-WHITESIDE
CHIEF HUMAN CAPITAL OFFICER AND DIRECTOR OF OPM HR

5-Part

2 - OPF Copy - Long-Term Record -- DO NOT DESTROY

Editions Prior to 7/91 Are Not Usable After 6/30/93
NSN 7540-01-333-6236

NOTICE TO EMPLOYEE

This is your copy of the official notice of a personnel action. Keep it with your records because it could be used to make employment, pay, and qualifications decisions about you in the future.

The Action

- Blocks 5-B and 6-B describe the personnel action(s) that occurred.
- Blocks 15-22 show the position and organization to which you are assigned.

Pay

- When the personnel action is an award or bonus, block 20 shows the amount of that one-time cash payment. When the action is not an award or bonus, block 12 shows your former total annual salary, and block 20 shows your new total annual salary (block 20C plus 20D). The amounts in blocks 12 and 20 do not include any one-time cash payments (such as performance awards and recruitment or relocation bonuses) or payments that may vary from one pay period to the next (such as overtime pay), or other forms of premium pay.
- Block 20A is the scheduled amount for your grade and step, including any special salary rate you receive. It does not include any locality-based pay. This rate of pay serves as the basis for determining your rate of pay upon promotion, change to a lower grade, or reassignment, and is used for pay retention purposes.
- Block 20B is the annual dollar amount of your interim Geographic Adjustment or, beginning in 1994, your locality-based comparability payment.
- Block 20C is your Adjusted Basic Pay, the total of blocks 20A and 20B. It serves as the basis for computing your retirement benefits, life insurance, premium pay, and severance pay.
- Block 20D is the total dollar amount of any Retention Allowances, Supervisory Differentials, and Staffing Differentials that are listed in the remarks block. These payments are made in the same manner as basic pay, but are not a part of basic pay for any purpose.

Block 24 - Tenure

- Identifies the nature of your appointment and is used to determine your rights during a reduction in force (RIF). Tenure groups are explained in more detail in subchapter 26 of FPM Supplement 296-33 and RIF is explained in FPM Supplement 351-1; both should be available for review in your personnel office.

Block 26 - Veterans Preference to RIF

- Indicates whether you have preference for reduction-in-force purposes.

Block 30 - Retirement Plan

- **FICA** - Social Security System
- **CS** - Civil Service Retirement System
- **CS-Spec** - Civil Service Retirement System for law enforcement and firefighter personnel
- **FS** - Foreign Service Retirement and Disability System
- **FERS** - Federal Employees' Retirement System
- **FERS-Reserve Tech** - Federal Employees' Retirement System for National Guard Reserve Technicians
- **FERS-ATC** - Federal Employees' Retirement System for Air Traffic Controllers
- **FERS-Spec** - Federal Employees' Retirement System for law enforcement and firefighter personnel
- **FSPS** - Foreign Service Pension System

Block 31 - Service computation Date (Leave)

- Shows when your Federal service began unless you have prior creditable service. If so, this date is constructed to include your total years, months and days of prior creditable civilian and military service.
- Full-time employees with fewer than 3 years of service earn 4 hours of annual leave each pay period; those with 3 or more years but less than 15 years earn 6 hours each pay period; and those with 15 or more years earn 8 hours each pay period.
- Your earnings and leave statement or your time and attendance card will

Block 32 - Work Schedule

- Your work schedule is established by your supervisor.
- A full-time employee works on a prearranged scheduled tour of duty that is usually 40 hours per week. A part-time employee has a prearranged scheduled tour of duty that is usually between 16 and 32 hours per week. An intermittent employee has no prearranged scheduled tour of duty and works when needed.
  Full-Time and part-time employees whose appointments are for 90 days or more are usually eligible to earn annual leave; intermittent employees are not.
  Seasonal employees work on an annually recurring bases for periods of less than 12 months each year; they may have a full-time, a part-time, or an intermittent schedule during their work season.
  On-call employees work during periods of heavy workload and are in pay status for at least 6 months of each year; they may have either a full-time or a part-time schedule when they are in pay status.

Block 33 - Part-time Hours Per Biweekly Pay Period

Indicates the number of hours a part-time employee is scheduled to work during a two-week pay period.

Block 34 - Position Occupied

Identifies the employment system under which you are serving -- the Competitive Service, the Excepted Service, or the Senior Executive Service (SES).
The employment system determines your eligibility to move to other jobs in the Federal service, your rights in disciplinary and adverse actions, and your eligibility for reemployment if you have Federal service.

Block 35 - FLSA Category

Exempt employees are not covered by the minimum wage and overtime law (the Fair Labor Standards Act); nonexempt employees are covered.

Block 37 - Bargaining Unit Status

Identifies a bargaining unit to which you belong, whether or not your are actually a member of a labor organization. Code "7777" indicates you are eligible but not in a bargaining unit; code "8888" indicates you are ineligible for inclusion in a bargaining unit.

Block 38 and 39 - Duty Station

Identifies the city, county, and state or the overseas location, where you actually work.

OTHER INFORMATION

- If your appointment entitles you to elect health benefits or life insurance, and you have not been provided materials explaining the programs available and the enrollment forms, contact your personnel specialist.
- Your personnel specialist will also tell you if your position is covered by an agreement between an employee organization (union) and your agency. If you are eligible to and elect to join an employee organization, you can elect to have your dues withheld from your salary.
- If you have questions or need more information about your rights and benefits, ask your supervisor or your personnel office.
- Definitions for any coded data in Blocks 1-24, 27-39 and 45-50 may be found in Federal Personnel Manual Supplement 292-1.

It is your responsibility to read all the information on the front of this notice and tell your personnel office immediately if there is an error in it.

Standard Form 50
Rev. 7/91
U.S. Office of Personnel Management
FPM Supp. 296-33, Subch. 4

NOTIFICATION OF PERSONNEL ACTION

1. Name (Last, First, Middle) HOGAN, GREGORY JOHN	2. Social Security Number [redacted]	3. Date of Birth [redacted]	4. Effective Date 02/11/2025

FIRST ACTION		SECOND ACTION	
5-A. Code 546	5-B. Nature of Action CONV TO SES NONCAREER APPT	6-A. Code	6-B. Nature of Action
5-C. Code V4L	5-D. Legal Authority 5 U.S.C. 3394(A).	6-C. Code	6-D. Legal Authority
5-E. Code AWM	5-F. Legal Authority OPM FORM 1652 DATED 02-11-2025	6-E. Code	6-F. Legal Authority

7. FROM: Position Title and Number
SENIOR ADVISOR TO THE DIRECTOR FOR TECHNOLOGY AND DELIVERY
PD: 6A38081

15. TO: Position Title and Number
CHIEF INFORMATION OFFICER
PD: 6A39566

8. Pay Plan	9. Occ. Code	10. Grade or Level	11. Step or Rate	12. Total Salary	13. Pay Basis	16. Pay Plan	17. Occ. Code	18. Grade or Level	19. Step or Rate	20. Total Salary/Award	21. Pay Basis
ES	0301	00	00	$195,200.00	PA	ES	0340	00	00	$195,200.00	PA

12A. Basic Pay	12B. Locality Adj.	12C. Adj. Basic Pay	12D. Other Pay	20A. Basic Pay	20B. Locality Adj.	20C. Adj. Basic Pay	20D. Other Pay
$195,200.00	$0	$195,200.00	$0	$195,200.00	$0	$195,200.00	$0

14. Name and Location of Position's Organization
OPM
OFC OF THE DIRECTOR
WASHINGTON DC

22. Name and Location of Position's Organization
OPM
OFC OF THE DIRECTOR
OFC OF THE CHIEF INFORMATION OFFICER
WASHINGTON DC

EMPLOYEE DATA

23. Veterans Preference: 1 (1 - None; 2 - 5 Point; 3 - 10 Point/Disability; 4 - 10 Point/Compensable; 5 - 10 Point/Other; 6 - 10 Point/Compensable/30%)	24. Tenure: 0 (0 - None; 1 - Permanent; 2 - Conditional; 3 - Indefinite)	25. Agency Use: JS	26. Veterans Pref for RIF: YES [✓ NO]
27. FEGLI: B0 [redacted]	28. Annuitant Indicator: 9 NOT APPLICABLE		29. Pay Rate Determinant: 0
30. Retirement Plan: KF [redacted]	31. Service Comp. Date (Leave): 01/20/2025	32. Work Schedule: F FULL TIME	33. Part-Time Hours Per Biweekly Pay Period:

POSITION DATA

34. Position Occupied: 3 (1 - Competitive Service; 2 - Excepted Service; 3 - SES General; 4 - SES Career)	35. FLSA Category: E (E - Exempt; N - Nonexempt)	36. Appropriation Code: 51AA0	37. Bargaining Unit Status: 8888
38. Duty Station Code: 11-0010-001	39. Duty Station (City - County - State or Overseas Location): WASHINGTON DISTRICT OF COLUMBIA DC		

40. AGENCY DATA	41.	42.	43.	44.
10068		0000	33.94	SPECIAL-SENSITIVE (SS)/HIGH RI

45. Remarks
APPROVED FOR CONVERSION TO PERMANENT INCUMBENCY ON 2-11-2025. OPM FORM 1652 DATED 02-11-2025.

46. Employing Department or Agency: OPM			50. Signature/Authentication and Title of Approving Official: ELECTRONICALLY SIGNED BY: CARMEN GARCIA-WHITESIDE CHIEF HUMAN CAPITAL OFFICER AND DIRECTOR OF OPM HR
47. Agency Code: OM00	48. Personnel Office ID: 1000	49. Approval Date: 02/18/2025	

5-Part **2 - OPF Copy - Long-Term Record -- DO NOT DESTROY**
Editions Prior to 7/91 Are Not Usable After 6/30/93
NSN 7540-01-333-6236

NOTICE TO EMPLOYEE

This is your copy of the official notice of a personnel action. Keep it with your records because it could be used to make employment, pay, and qualifications decisions about you in the future.

The Action

- Blocks 5-B and 6-B describe the personnel action(s) that occurred.
- Blocks 15-22 show the position and organization to which you are assigned.

Pay

- When the personnel action is an award or bonus, block 20 shows the amount of that one-time cash payment. When the action is not an award or bonus, block 12 shows your former total annual salary, and block 20 shows your new total annual salary (block 20C plus 20D). The amounts in blocks 12 and 20 do not include any one-time cash payments (such as performance awards and recruitment or relocation bonuses) or payments that may vary from one pay period to the next (such as overtime pay), or other forms of premium pay.
- Block 20A is the scheduled amount for your grade and step, including any special salary rate you receive. It does not include any locality-based pay. This rate of pay serves as the basis for determining your rate of pay upon promotion, change to a lower grade, or reassignment, and is used for pay retention purposes.
- Block 20B is the annual dollar amount of your interim Geographic Adjustment or, beginning in 1994, your locality-based comparability payment.
- Block 20C is your Adjusted Basic Pay, the total of blocks 20A and 20B. It serves as the basis for computing your retirement benefits, life insurance, premium pay, and severance pay.
- Block 20D is the total dollar amount of any Retention Allowances, Supervisory Differentials, and Staffing Differentials that are listed in the remarks block. These payments are made in the same manner as basic pay, but are not a part of basic pay for any purpose.

Block 24 - Tenure

- Identifies the nature of your appointment and is used to determine your rights during a reduction in force (RIF). Tenure groups are explained in more detail in subchapter 26 of FPM Supplement 296-33 and RIF is explained in FPM Supplement 351-1; both should be available for review in your personnel office.

Block 26 - Veterans Preference to RIF

- Indicates whether you have preference for reduction-in-force purposes.

Block 30 - Retirement Plan

- **FICA** - Social Security System
- **CS** - Civil Service Retirement System
- **CS-Spec** - Civil Service Retirement System for law enforcement and firefighter personnel
- **FS** - Foreign Service Retirement and Disability System
- **FERS** - Federal Employees' Retirement System
- **FERS-Reserve Tech** - Federal Employees' Retirement System for National Guard Reserve Technicians
- **FERS-ATC** - Federal Employees' Retirement System for Air Traffic Controllers
- **FERS-Spec** - Federal Employees' Retirement System for law enforcement and firefighter personnel
- **FSPS** - Foreign Service Pension System

Block 31 - Service computation Date (Leave)

- Shows when your Federal service began unless you have prior creditable service. If so, this date is constructed to include your total years, months and days of prior creditable civilian and military service.
- Full-time employees with fewer than 3 years of service earn 4 hours of annual leave each pay period; those with 3 or more years but less than 15 years earn 6 hours each pay period; and those with 15 or more years earn 8 hours each pay period.
- Your earnings and leave statement or your time and attendance card will

Block 32 - Work Schedule

- Your work schedule is established by your supervisor.
- A full-time employee works on a prearranged scheduled tour of duty that is usually 40 hours per week. A part-time employee has a prearranged scheduled tour of duty that is usually between 16 and 32 hours per week. An intermittent employee has no prearranged scheduled tour of duty and works when needed.
  Full-Time and part-time employees whose appointments are for 90 days or more are usually eligible to earn annual leave; intermittent employees are not.
  Seasonal employees work on an annually recurring bases for periods of less than 12 months each year; they may have a full-time, a part-time, or an intermittent schedule during their work season.
  On-call employees work during periods of heavy workload and are in pay status for at least 6 months of each year; they may have either a full-time or a part-time schedule when they are in pay status.

Block 33 - Part-time Hours Per Biweekly Pay Period

Indicates the number of hours a part-time employee is scheduled to work during a two-week pay period.

Block 34 - Position Occupied

Identifies the employment system under which you are serving -- the Competitive Service, the Excepted Service, or the Senior Executive Service (SES).
The employment system determines your eligibility to move to other jobs in the Federal service, your rights in disciplinary and adverse actions, and your eligibility for reemployment if you have Federal service.

Block 35 - FLSA Category

Exempt employees are not covered by the minimum wage and overtime law (the Fair Labor Standards Act); nonexempt employees are covered.

Block 37 - Bargaining Unit Status

Identifies a bargaining unit to which you belong, whether or not your are actually a member of a labor organization. Code "7777" indicates you are eligible but not in a bargaining unit; code "8888" indicates you are ineligible for inclusion in a bargaining unit.

Block 38 and 39 - Duty Station

Identifies the city, county, and state or the overseas location, where you actually work.

OTHER INFORMATION

- If your appointment entitles you to elect health benefits or life insurance, and you have not been provided materials explaining the programs available and the enrollment forms, contact your personnel specialist.
- Your personnel specialist will also tell you if your position is covered by an agreement between an employee organization (union) and your agency. If you are eligible to and elect to join an employee organization, you can elect to have your dues withheld from your salary.
- If you have questions or need more information about your rights and benefits, ask your supervisor or your personnel office.
- Definitions for any coded data in Blocks 1-24, 27-39 and 45-50 may be found in Federal Personnel Manual Supplement 292-1.

It is your responsibility to read all the information on the front of this notice and tell your personnel office immediately if there is an error in it.

APPOINTMENT AFFIDAVITS

Senior Advisor	01/20/2025
(Position to which Appointed)	(Date Appointed)

Office of Personnel Managemer	Office of the Director	Washington, D.C.
(Department or Agency)	(Bureau or Division)	(Place of Employment)

I, OPM-2, do solemnly swear (or affirm) that--

A. OATH OF OFFICE

I will support and defend the Constitution of the United States against all enemies, foreign and domestic; that I will bear true faith and allegiance to the same; that I take this obligation freely, without any mental reservation or purpose of evasion; and that I will well and faithfully discharge the duties of the office on which I am about to enter. So help me God.

B. AFFIDAVIT AS TO STRIKING AGAINST THE FEDERAL GOVERNMENT

I am not participating in any strike against the Government of the United States or any agency thereof, and I will not so participate while an employee of the Government of the United States or any agency thereof.

C. AFFIDAVIT AS TO THE PURCHASE AND SALE OF OFFICE

I have not, nor has anyone acting in my behalf, given, transferred, promised or paid any consideration for or in expectation or hope of receiving assistance in securing this appointment.

OPM-2
50AC0E749A494TC...
(Signature of Appointee)

Subscribed and sworn (or affirmed) before me this 20 day of January, 2025

at Washington (City) DC (State)

[illegible]
(Signature of Officer)

(SEAL)

Commission expires ____________
(If by a Notary Public, the date of his/her Commission should be shown)

Acting Director
(Title)

Note - If the appointee objects to the form of the oath on religious grounds, certain modifications may be permitted pursuant to the Religious Freedom Restoration Act. Please contact your agency's legal counsel for advice.

Acceptance of Uncompensated Services

I understand that I may be employed with the United States Office of Personnel Management (OPM) under the authority of 5 U.S.C. § 3109. Under certain circumstances, OPM may use this authority to employ experts or consultants with or without pay, provided that such personnel agree in advance in writing to waive any claims for compensation for those services.

I desire to offer my services to OPM. Accordingly, I agree to being appointed as an uncompensated employee of OPM; I understand that I will not receive any pay or any other form of compensation from OPM, the federal Government, or any other source for the services I render to OPM.

In addition, I hereby waive any and all claims I may have in the future against OPM and/or the federal Government on account of the services I render to OPM.

Signed: __**OPM-2**__________________________________
50AC0E749AA941C...

Printed Name of Appointee: _____ **OPM-2** ____________________________

Date: January 20, 2025

Standard Form 50
Rev. 7/91
U.S. Office of Personnel Management
FPM Supp. 296-33, Subch. 4

NOTIFICATION OF PERSONNEL ACTION

1. Name (Last, First, Middle) OPM-2	2. Social Security Number [redacted]	3. Date of Birth [redacted]	4. Effective Date 01/20/2025

FIRST ACTION

5-A. Code 171	5-B. Nature of Action EXC APPT NTE 07/18/2025
5-C. Code H2L	5-D. Legal Authority REG 304.103.
5-E. Code	5-F. Legal Authority

SECOND ACTION

6-A. Code	6-B. Nature of Action
6-C. Code	6-D. Legal Authority
6-E. Code	6-F. Legal Authority

7. FROM: Position Title and Number

8. Pay Plan	9. Occ. Code	10. Grade or Level	11. Step or Rate	12. Total Salary	13. Pay Basis

12A. Basic Pay	12B. Locality Adj.	12C. Adj. Basic Pay	12D. Other Pay

14. Name and Location of Position's Organization

15. TO: Position Title and Number
EXPERT
PD: 6A39741

16. Pay Plan	17. Occ. Code	18. Grade or Level	19. Step or Rate	20. Total Salary/Award	21. Pay Basis
ED	0301	00	00	$0	WC

20A. Basic Pay	20B. Locality Adj.	20C. Adj. Basic Pay	20D. Other Pay
$0	$0	$0	$0

22. Name and Location of Position's Organization
OPM
OFC OF THE DIRECTOR

WASHINGTON DC

EMPLOYEE DATA

23. Veterans Preference: 1 — 1 None; 2 5-Point; 3 10-Point/Disability; 4 10-Point/Compensable; 5 10-Point/Other; 6 10-Point/Compensable/30%

24. Tenure: 0 — 0 None; 1 Permanent; 2 Conditional; 3 Indefinite

25. Agency Use: TG

26. Veterans Pref for RIF: YES [✓ NO]

27. FEGLI: A0 [redacted]

28. Annuitant Indicator: 9 NOT APPLICABLE

29. Pay Rate Determinant: 0

30. Retirement Plan: 4 [redacted]

31. Service Comp. Date (Leave): 01/20/2025

32. Work Schedule: F FULL TIME

33. Part-Time Hours Per Biweekly Pay Period:

POSITION DATA

34. Position Occupied: 2 — 1 Competitive Service; 2 Excepted Service; 3 SES General; 4 SES Career

35. FLSA Category: E — E Exempt; N Nonexempt

36. Appropriation Code: 41AA0

37. Bargaining Unit Status: 8888

38. Duty Station Code: 11-0010-001

39. Duty Station (City - County - State or Overseas Location): WASHINGTON DISTRICT OF COLUMBIA DC

40. AGENCY DATA	41.	42.	43.	44.
10001		0000	33.94	CRITICAL-SENSITIVE (CS)/HIGH R

45. Remarks

APPOINTMENT AFFIDAVIT EXECUTED 01-20-2025

REASON FOR TEMPORARY APPOINTMENT: TO PROVIDE A HIGH LEVEL OF EXPERTISE RELATIVE TO ISSUES WHICH HAVE A SIGNIFICANT IMPACT ON THE FORMULATION OF AGENCY GOALS AND OBJECTIVES TO THE OPM DIRECTOR.

CREDITABLE MILITARY SERVICE: 0000

PREVIOUS RETIREMENT COVERAGE: NEVER COVERED

46. Employing Department or Agency: OPM

47. Agency Code	48. Personnel Office ID	49. Approval Date
OM00	1000	01/30/2025

50. Signature/Authentication and Title of Approving Official
ELECTRONICALLY SIGNED BY:
CARMEN GARCIA-WHITESIDE
CHIEF HUMAN CAPITAL OFFICER AND DIRECTOR OF OPM HR

5-Part **2 - OPF Copy - Long-Term Record -- DO NOT DESTROY**

Editions Prior to 7/91 Are Not Usable After 6/30/93
NSN 7540-01-333-6236

NOTICE TO EMPLOYEE

This is your copy of the official notice of a personnel action. Keep it with your records because it could be used to make employment, pay, and qualifications decisions about you in the future.

The Action

- Blocks 5-B and 6-B describe the personnel action(s) that occurred.
- Blocks 15-22 show the position and organization to which you are assigned.

Pay

- When the personnel action is an award or bonus, block 20 shows the amount of that one-time cash payment. When the action is not an award or bonus, block 12 shows your former total annual salary, and block 20 shows your new total annual salary (block 20C plus 20D). The amounts in blocks 12 and 20 do not include any one-time cash payments (such as performance awards and recruitment or relocation bonuses) or payments that may vary from one pay period to the next (such as overtime pay), or other forms of premium pay.
- Block 20A is the scheduled amount for your grade and step, including any special salary rate you receive. It does not include any locality-based pay. This rate of pay serves as the basis for determining your rate of pay upon promotion, change to a lower grade, or reassignment, and is used for pay retention purposes.
- Block 20B is the annual dollar amount of your interim Geographic Adjustment or, beginning in 1994, your locality-based comparability payment.
- Block 20C is your Adjusted Basic Pay, the total of blocks 20A and 20B. It serves as the basis for computing your retirement benefits, life insurance, premium pay, and severance pay.
- Block 20D is the total dollar amount of any Retention Allowances, Supervisory Differentials, and Staffing Differentials that are listed in the remarks block. These payments are made in the same manner as basic pay, but are not a part of basic pay for any purpose.

Block 24 - Tenure

- Identifies the nature of your appointment and is used to determine your rights during a reduction in force (RIF). Tenure groups are explained in more detail in subchapter 26 of FPM Supplement 296-33 and RIF is explained in FPM Supplement 351-1; both should be available for review in your personnel office.

Block 26 - Veterans Preference to RIF

- Indicates whether you have preference for reduction-in-force purposes.

Block 30 - Retirement Plan

- **FICA** - Social Security System
- **CS** - Civil Service Retirement System
- **CS-Spec** - Civil Service Retirement System for law enforcement and firefighter personnel
- **FS** - Foreign Service Retirement and Disability System
- **FERS** - Federal Employees' Retirement System
- **FERS-Reserve Tech** - Federal Employees' Retirement System for National Guard Reserve Technicians
- **FERS-ATC** - Federal Employees' Retirement System for Air Traffic Controllers
- **FERS-Spec** - Federal Employees' Retirement System for law enforcement and firefighter personnel
- **FSPS** - Foreign Service Pension System

Block 31 - Service computation Date (Leave)

- Shows when your Federal service began unless you have prior creditable service. If so, this date is constructed to include your total years, months and days of prior creditable civilian and military service.
- Full-time employees with fewer than 3 years of service earn 4 hours of annual leave each pay period; those with 3 or more years but less than 15 years earn 6 hours each pay period; and those with 15 or more years earn 8 hours each pay period.
- Your earnings and leave statement or your time and attendance card will

Block 32 - Work Schedule

- Your work schedule is established by your supervisor.
- A full-time employee works on a prearranged scheduled tour of duty that is usually 40 hours per week. A part-time employee has a prearranged scheduled tour of duty that is usually between 16 and 32 hours per week. An intermittent employee has no prearranged scheduled tour of duty and works when needed.
  Full-Time and part-time employees whose appointments are for 90 days or more are usually eligible to earn annual leave; intermittent employees are not.
  Seasonal employees work on an annually recurring bases for periods of less than 12 months each year; they may have a full-time, a part-time, or an intermittent schedule during their work season.
  On-call employees work during periods of heavy workload and are in pay status for at least 6 months of each year; they may have either a full-time or a part-time schedule when they are in pay status.

Block 33 - Part-time Hours Per Biweekly Pay Period

Indicates the number of hours a part-time employee is scheduled to work during a two-week pay period.

Block 34 - Position Occupied

Identifies the employment system under which you are serving -- the Competitive Service, the Excepted Service, or the Senior Executive Service (SES).
The employment system determines your eligibility to move to other jobs in the Federal service, your rights in disciplinary and adverse actions, and your eligibility for reemployment if you have Federal service.

Block 35 - FLSA Category

Exempt employees are not covered by the minimum wage and overtime law (the Fair Labor Standards Act); nonexempt employees are covered.

Block 37 - Bargaining Unit Status

Identifies a bargaining unit to which you belong, whether or not your are actually a member of a labor organization. Code "7777" indicates you are eligible but not in a bargaining unit; code "8888" indicates you are ineligible for inclusion in a bargaining unit.

Block 38 and 39 - Duty Station

Identifies the city, county, and state or the overseas location, where you actually work.

OTHER INFORMATION

- If your appointment entitles you to elect health benefits or life insurance, and you have not been provided materials explaining the programs available and the enrollment forms, contact your personnel specialist.
- Your personnel specialist will also tell you if your position is covered by an agreement between an employee organization (union) and your agency. If you are eligible to and elect to join an employee organization, you can elect to have your dues withheld from your salary.
- If you have questions or need more information about your rights and benefits, ask your supervisor or your personnel office.
- Definitions for any coded data in Blocks 1-24, 27-39 and 45-50 may be found in Federal Personnel Manual Supplement 292-1.

It is your responsibility to read all the information on the front of this notice and tell your personnel office immediately if there is an error in it.

APPOINTMENT AFFIDAVITS

Expert	01/20/2025
(Position to which Appointed)	*(Date Appointed)*

Office of Personnel Managemer	Office of the Director	Washinton, D.C.
(Department or Agency)	*(Bureau or Division)*	*(Place of Employment)*

I, **OPM-3** ____________________, do solemnly swear (or affirm) that--

A. OATH OF OFFICE

I will support and defend the Constitution of the United States against all enemies, foreign and domestic; that I will bear true faith and allegiance to the same; that I take this obligation freely, without any mental reservation or purpose of evasion; and that I will well and faithfully discharge the duties of the office on which I am about to enter. So help me God.

B. AFFIDAVIT AS TO STRIKING AGAINST THE FEDERAL GOVERNMENT

I am not participating in any strike against the Government of the United States or any agency thereof, and I will not so participate while an employee of the Government of the United States or any agency thereof.

C. AFFIDAVIT AS TO THE PURCHASE AND SALE OF OFFICE

I have not, nor has anyone acting in my behalf, given, transferred, promised or paid any consideration for or in expectation or hope of receiving assistance in securing this appointment.

OPM-3
(Signature of Appointee)

Subscribed and sworn (or affirmed) before me this 20 day of Jana ry, 2025

at Washington (City) D.C. (State)

[illegible]
(Signature of Officer)

(SEAL)

Commission expires__________
(If by a Notary Public, the date of his/her Commission should be shown)

Acting Director
(Title)

Note - If the appointee objects to the form of the oath on religious grounds, certain modifications may be permitted pursuant to the Religious Freedom Restoration Act. Please contact your agency's legal counsel for advice.

Standard Form 50
Rev. 7/91
U.S. Office of Personnel Management
FPM Supp. 296-33, Subch. 4

NOTIFICATION OF PERSONNEL ACTION

1. Name (Last, First, Middle) OPM-3	2. Social Security Number [redacted]	3. Date of Birth [redacted]	4. Effective Date 01/20/2025

FIRST ACTION

5-A. Code 171	5-B. Nature of Action EXC APPT NTE 07/18/2025
5-C. Code H2L	5-D. Legal Authority REG 304.103.
5-E. Code	5-F. Legal Authority

SECOND ACTION

6-A. Code	6-B. Nature of Action
6-C. Code	6-D. Legal Authority
6-E. Code	6-F. Legal Authority

7. FROM: Position Title and Number

8. Pay Plan	9. Occ. Code	10. Grade or Level	11. Step or Rate	12. Total Salary	13. Pay Basis

12A. Basic Pay	12B. Locality Adj.	12C. Adj. Basic Pay	12D. Other Pay

14. Name and Location of Position's Organization

15. TO: Position Title and Number
EXPERT
PD: 6A39740

16. Pay Plan	17. Occ. Code	18. Grade or Level	19. Step or Rate	20. Total Salary/Award	21. Pay Basis
ED	0301	00	00	$0	WC

20A. Basic Pay	20B. Locality Adj.	20C. Adj. Basic Pay	20D. Other Pay
$0	$0	$0	$0

22. Name and Location of Position's Organization
OPM
OFC OF THE DIRECTOR

WASHINGTON DC

EMPLOYEE DATA

23. Veterans Preference: 1 (1 - None; 2 - 5 Point; 3 - 10 Point/Disability; 4 - 10 Point/Compensable; 5 - 10 Point/Other; 6 - 10 Point/Compensable/30%)

24. Tenure: 0 (0 - None; 1 - Permanent; 2 - Conditional; 3 - Indefinite)

25. Agency Use: TG

26. Veterans Preference for RIF: YES [✓ X NO]

27. FEGLI: A0 [redacted]

28. Annuitant Indicator: 9 NOT APPLICABLE

29. Pay Rate Determinant: 0

30. Retirement Plan: 4 [redacted]

31. Service Comp. Date (Leave): 01/20/2025

32. Work Schedule: F FULL TIME

33. Part-Time Hours Per Biweekly Pay Period:

POSITION DATA

34. Position Occupied: 2 (1 - Competitive Service; 2 - Excepted Service; 3 - SES General; 4 - SES Career Reserved)

35. FLSA Category: E (E - Exempt; N - Nonexempt)

36. Appropriation Code: 41AA0

37. Bargaining Unit Status: 8888

38. Duty Station Code: 11-0010-001

39. Duty Station (City - County - State or Overseas Location): WASHINGTON DISTRICT OF COLUMBIA DC

40. Agency Data	41.	42.	43.	44.
10001		0000	33.94	CRITICAL-SENSITIVE (CS)/HIGH R

45. Remarks
```
APPOINTMENT AFFIDAVIT EXECUTED 01/20/2025
REASON FOR TEMPORARY APPOINTMENT: TO PROVIDE A HIGH LEVEL OF EXPERTISE RELATIVE TO ISSUES WHICH HAVE A
 SIGNIFICANT IMPACT ON THE FORMULATION OF AGENCY GOALS AND OBJECTIVES TO THE OPM DIRECTOR.
CREDITABLE MILITARY SERVICE: 0000
PREVIOUS RETIREMENT COVERAGE:  NEVER COVERED.
```

46. Employing Department or Agency: OPM

47. Agency Code	48. Personnel Office ID	49. Approval Date
OM00	1000	01/30/2025

50. Signature/Authentication and Title of Approving Official
ELECTRONICALLY SIGNED BY:
CARMEN GARCIA-WHITESIDE
CHIEF HUMAN CAPITAL OFFICER AND DIRECTOR OF OPM HR

5-Part 50-316

2 - OPF Copy - Long-Term Record - DO NOT DESTROY

Editions Prior to 7/91 Are Not Usable After 6/30/93
NSN 7540-01-333-6238

Acceptance of Uncompensated Services

I understand that I may be employed with the United States Office of Personnel Management (OPM) under the authority of 5 U.S.C. § 3109. Under certain circumstances, OPM may use this authority to employ experts or consultants with or without pay, provided that such personnel agree in advance in writing to waive any claims for compensation for those services.

I desire to offer my services to OPM. Accordingly, I agree to being appointed as an uncompensated employee of OPM; I understand that I will not receive any pay or any other form of compensation from OPM, the federal Government, or any other source for the services I render to OPM.

In addition, I hereby waive any and all claims I may have in the future against OPM and/or the federal Government on account of the services I render to OPM.

Signed: **OPM-3**

Printed Name of Appointee: **OPM-3**

Date: January 28, 2025

2/12/25

MEMORANDUM OF UNDERSTANDING BETWEEN THE SOCIAL SECURITY ADMINISTRATION, THE OFFICE OF PERSONNEL MANAGEMENT, THE DEPARTMENT OF EDUCATION, AND APPOINTEE OPM-3

During Appointee's term of service at the Social Security Administration (SSA), Appointee may also serve as an unpaid Special Government Employee (SGE) for the Office of Personnel Management (OPM) and the Department of Education . The Appointees duties, qualifications, and salary are contained in the attached Expert or Consultant Appointment Request & Certification (Appointment Request and Certification). To ensure compliance with applicable law, the Appointee, OPM, the Department of Education (DoEd.), and SSA (the parties) enter into this Memorandum of Understanding (MOU) and agree as follows:

1. During Appointee's term of service to SSA, Appointee will receive payment, as described in the Appointment Request and Certification, from SSA.
2. Neither OPM nor DoEd. shall not pay Appointee during his SSA term of service.
3. While on duty time at SSA, Appointee shall only perform duties for SSA.
4. While on duty time at SSA, Appointee shall not perform any work for or on behalf of OPM or DoEd..
5. Appointee shall perform SSA work only at SSA Headquarters (HQ) in Woodlawn, Maryland.
6. Appointee shall not perform any work for OPM or DoEd.at SSA facilities, including but not limited to SSA HQ.
7. SSA, OPM and DoEd. shall provide any equipment or systems access to ensure access to their respective networks. Neither SSA, OPM nor DoEd. shall be responsible for providing access to the other agency's network or systems.
8. Appointee shall not perform work for either OPM or DoEd. using SSA equipment or resources.
9. Appointee shall not perform SSA work using either OPM or DoEd. equipment or resources.
10. Appointee shall not share any Personally Identifiable Information accessed or obtained through the use of SSA systems or work performed for SSA, with any external entity, organization, or agency federal or state, including OPM and DoEd.
11. Appointee shall not share or disclose SSA information that is non- PII, non-public information with any non-federal entity. Any disclosure of non- PII, non-public information to another federal entity, organization, or agency shall be made only with expressed permission of the Office of the Commissioner.
12. Appointee shall not share or disclose OPM or DoEd. information to SSA without appropriate permission from each agency's appropriate authorizing official.
13. Appointee shall abide by all SSA regulations and policies regarding access to and protection of any agency records, information, and work products.
14. Appointee shall abide all SSA regulations and policies regarding ethics and employee conduct.
15. In the event of any lapse in appropriations, the Appointee will follow the instructions issued by SSA related to his SSA service.

AUTHORIZING SIGNATURES AND DATES

The signatories below warrant and represent that they have the competent authority on behalf of their respective agencies to enter into the obligations set forth in this MOU. This agreement will become effective on the date it is signed by last party.

Social Security Administration

Florence Felix-Lawson

[NAME] Florence Felix-Lawson
[TITLE] Chief Human Capital Officer
Social Security Administration

Date: 2/13/25

Office of Personnel Management

Brian Bjelde

[NAME] Brian Bjelde
[TITLE] Senior Advisor to Acting Director of OPM

Date: 2/12/2025

Department of Education

[illegible]

James P. Bergeron
Acting Under Secretary

Date: 02/12/25

Appointee

OPM-3

Akash Bobba

Date: 02/12/2025

APPOINTMENT AFFIDAVITS

Expert	01/24/2025
(Position to which Appointed)	*(Date Appointed)*

Office of Personnel Managemer	Office of the Director	Washington, D.C.
(Department or Agency)	*(Bureau or Division)*	*(Place of Employment)*

I, OPM-4, do solemnly swear (or affirm) that--

A. OATH OF OFFICE

I will support and defend the Constitution of the United States against all enemies, foreign and domestic; that I will bear true faith and allegiance to the same; that I take this obligation freely, without any mental reservation or purpose of evasion; and that I will well and faithfully discharge the duties of the office on which I am about to enter. So help me God.

B. AFFIDAVIT AS TO STRIKING AGAINST THE FEDERAL GOVERNMENT

I am not participating in any strike against the Government of the United States or any agency thereof, and I will not so participate while an employee of the Government of the United States or any agency thereof.

C. AFFIDAVIT AS TO THE PURCHASE AND SALE OF OFFICE

I have not, nor has anyone acting in my behalf, given, transferred, promised or paid any consideration for or in expectation or hope of receiving assistance in securing this appointment.

OPM-4

(Signature of Appointee)

Subscribed and sworn (or affirmed) before me this 24 day of JANUARY, 2025

at WASHINGTON (City) D.C. (State)

[illegible]
(Signature of Officer)

(SEAL)

Commission expires ____________
(If by a Notary Public, the date of his/her Commission should be shown)

SUPERVISORY HR SPECIALIST
(Title)

Note - If the appointee objects to the form of the oath on religious grounds, certain modifications may be permitted pursuant to the Religious Freedom Restoration Act. Please contact your agency's legal counsel for advice.

U.S. Office of Personnel Management
The Guide to Processing Personnel Actions

NSN 7540-00-634-4015

Standard Form 61
Revised August 2002
Previous editions not usable

Acceptance of Uncompensated Services

I understand that I may be employed with the United States Office of Personnel Management (OPM) under the authority of 5 U.S.C. § 3109. Under certain circumstances, OPM may use this authority to employ experts or consultants with or without pay, provided that such personnel agree in advance in writing to waive any claims for compensation for those services.

I desire to offer my services to OPM. Accordingly, I agree to being appointed as an uncompensated employee of OPM; I understand that I will not receive any pay or any other form of compensation from OPM, the federal Government, or any other source for the services I render to OPM.

In addition, I hereby waive any and all claims I may have in the future against OPM and/or the federal Government on account of the services I render to OPM.

Signed: **OPM-4**

Printed Name of Appointee: **OPM-4**

Date: January 24, 2025

APPOINTMENT AFFIDAVITS

Senior Advisor to the Director
(Position to which Appointed)

01/20/2025
(Date Appointed)

Office of Personnel Management
(Department or Agency)

Office of the Director
(Bureau or Division)

Washington, DC, United States
(Place of Employment)

I, OPM-5, do solemnly swear (or affirm) that–

A. OATH OF OFFICE

I will support and defend the Constitution of the United States against all enemies, foreign and domestic; that I will bear true faith and allegiance to the same; that I take this obligation freely, without any mental reservation or purpose of evasion; and that I will well and faithfully discharge the duties of the office on which I am about to enter. So help me God.

B. AFFIDAVIT AS TO STRIKING AGAINST THE FEDERAL GOVERNMENT

I am not participating in any strike against the Government of the United States or any agency thereof, and I will not so participate while an employee of the Government of the United States or any agency thereof.

C. AFFIDAVIT AS TO THE PURCHASE AND SALE OF OFFICE

I have not, nor has anyone acting in my behalf, given, transferred, promised or paid any consideration for or in expectation or hope of receiving assistance in securing this appointment.

OPM-5
(Signature of Appointee)

Subscribed and sworn (or affirmed) before me this 20 day of January, 2025

at Washington (City) DC (State)

[illegible]
(Signature of Officer)

(SEAL)

Commission expires ________
(If by a Notary Public, the date of his/her Commission should be shown)

Acting Director
(Title)

Note - If the appointee objects to the form of the oath on religious grounds, certain modifications may be permitted pursuant to the Religious Freedom Restoration Act. Please contact your agency's legal counsel for advice.

Standard Form 50
Rev. 7/91
U.S. Office of Personnel Management
FPM Supp. 296-33, Subch. 4

NOTIFICATION OF PERSONNEL ACTION

1. Name (Last, First, Middle)	2. Social Security Number	3. Date of Birth	4. Effective Date
OPM-5	[redacted]	[redacted]	01/20/2025

FIRST ACTION

5-A. Code	5-B. Nature of Action
190	PROVISIONAL APPT NTE 05/20/2025
5-C. Code	**5-D. Legal Authority**
Y9K	SCH C, 213.3302(A).
5-E. Code	**5-F. Legal Authority**
AWM	OPM FORM 1019 DATED 01-20-2025

SECOND ACTION

6-A. Code	6-B. Nature of Action
6-C. Code	**6-D. Legal Authority**
6-E. Code	**6-F. Legal Authority**

7. FROM: Position Title and Number

8. Pay Plan	9. Occ. Code	10. Grade or Level	11. Step or Rate	12. Total Salary	13. Pay Basis

12A. Basic Pay	12B. Locality Adj.	12C. Adj. Basic Pay	12D. Other Pay

14. Name and Location of Position's Organization

15. TO: Position Title and Number
SENIOR ADVISOR TO THE DIRECTOR FOR INFORMATION TECHNOLOGY
PD 6A38025

16. Pay Plan	17. Occ. Code	18. Grade or Level	19. Step or Rate	20. Total Salary/Award	21. Pay Basis
GS	0301	15	10	$195,200.00	PA

20A. Basic Pay	20B. Locality Adj.	20C. Adj. Basic Pay	20D. Other Pay
$162,672.00	$32,528.00	$195,200.00	$0

22. Name and Location of Position's Organization
OPM
OFC OF THE DIRECTOR

WASHINGTON DC

EMPLOYEE DATA

23. Veterans Preference: 1
1 - None; 2 - 5 Point; 3 - 10 Point/Disability; 4 - 10 Point/Compensable; 5 - 10 Point/Other; 6 - 10 Point/Compensable/30%

24. Tenure: 3
0 - None; 1 - Permanent; 2 - Conditional; 3 - Indefinite

25. Agency Use: MK

26. Veterans Pref for RIF: YES [✓ NO]

27. FEGLI: C0 [redacted]

28. Annuitant Indicator: 9 NOT APPLICABLE

29. Pay Rate Determinant: 7

30. Retirement Plan: KF [redacted]

31. Service Comp. Date (Leave): 01/20/2025

32. Work Schedule: F FULL TIME

33. Part-Time Hours Per Biweekly Pay Period:

POSITION DATA

34. Position Occupied: 2
1 - Competitive Service; 2 - Excepted Service; 3 - SES General; 4 - SES Career

35. FLSA Category: E
E - Exempt; N - Nonexempt

36. Appropriation Code: 41AA0

37. Bargaining Unit Status: 8888

38. Duty Station Code: 11-0010-001

39. Duty Station (City - County - State or Overseas Location): WASHINGTON DISTRICT OF COLUMBIA DC

40. AGENCY DATA	41.	42.	43.	44.
10001		0000	33.94	CRITICAL-SENSITIVE (CS)/HIGH R

45. Remarks

APPOINTMENT IS INDEFINITE.

APPOINTMENT IS ON A PROVISIONAL BASIS. YOU ARE ELIGIBLE FOR RETIREMENT COVERAGE AND FOR HEALTH BENEFITS AND LIFE INSURANCE. IF YOUR PERFORMANCE IS SATISFACTORY, AND YOU MEET ALL LEGAL, QUALIFICATIONS, AND OTHER APPLICABLE REQUIREMENTS, YOU MAY BE CONVERTED TO A NONTEMPORARY APPOINTMENT BEFORE THIS APPOINTMENT EXPIRES.

APPOINTMENT AFFIDAVIT EXECUTED 01-20-2025.

CREDITABLE MILITARY SERVICE: 0000

PREVIOUS RETIREMENT COVERAGE: NEVER COVERED

EMPLOYEE IS AUTOMATICALLY COVERED UNDER FERS, FERS-RAE, OR FERS-FRAE.

OPM FORM 1019 DATED 01-20-2025.

46. Employing Department or Agency: OPM

47. Agency Code	48. Personnel Office ID	49. Approval Date
OM00	1000	01/27/2025

50. Signature/Authentication and Title of Approving Official
ELECTRONICALLY SIGNED BY:
CARMEN GARCIA-WHITESIDE
CHIEF HUMAN CAPITAL OFFICER AND DIRECTOR OF OPM HR

5-Part **2 - OPF Copy - Long-Term Record -- DO NOT DESTROY**

Editions Prior to 7/91 Are Not Usable After 6/30/93
NSN 7540-01-333-6236

NOTICE TO EMPLOYEE

This is your copy of the official notice of a personnel action. Keep it with your records because it could be used to make employment, pay, and qualifications decisions about you in the future.

The Action

- Blocks 5-B and 6-B describe the personnel action(s) that occurred.
- Blocks 15-22 show the position and organization to which you are assigned.

Pay

- When the personnel action is an award or bonus, block 20 shows the amount of that one-time cash payment. When the action is not an award or bonus, block 12 shows your former total annual salary, and block 20 shows your new total annual salary (block 20C plus 20D). The amounts in blocks 12 and 20 do not include any one-time cash payments (such as performance awards and recruitment or relocation bonuses) or payments that may vary from one pay period to the next (such as overtime pay), or other forms of premium pay.
- Block 20A is the scheduled amount for your grade and step, including any special salary rate you receive. It does not include any locality-based pay. This rate of pay serves as the basis for determining your rate of pay upon promotion, change to a lower grade, or reassignment, and is used for pay retention purposes.
- Block 20B is the annual dollar amount of your interim Geographic Adjustment or, beginning in 1994, your locality-based comparability payment.
- Block 20C is your Adjusted Basic Pay, the total of blocks 20A and 20B. It serves as the basis for computing your retirement benefits, life insurance, premium pay, and severance pay.
- Block 20D is the total dollar amount of any Retention Allowances, Supervisory Differentials, and Staffing Differentials that are listed in the remarks block. These payments are made in the same manner as basic pay, but are not a part of basic pay for any purpose.

Block 24 - Tenure

- Identifies the nature of your appointment and is used to determine your rights during a reduction in force (RIF). Tenure groups are explained in more detail in subchapter 26 of FPM Supplement 296-33 and RIF is explained in FPM Supplement 351 1; both should be available for review in your personnel office.

Block 26 - Veterans Preference to RIF

- Indicates whether you have preference for reduction-in-force purposes.

Block 30 - Retirement Plan

- **FICA** - Social Security System
- **CS** - Civil Service Retirement System
- **CS-Spec** - Civil Service Retirement System for law enforcement and firefighter personnel
- **FS** - Foreign Service Retirement and Disability System
- **FERS** - Federal Employees' Retirement System
- **FERS-Reserve Tech** - Federal Employees' Retirement System for National Guard Reserve Technicians
- **FERS-ATC** - Federal Employees' Retirement System for Air Traffic Controllers
- **FERS-Spec** - Federal Employees' Retirement System for law enforcement and firefighter personnel
- **FSPS** - Foreign Service Pension System

Block 31 - Service computation Date (Leave)

- Shows when your Federal service began unless you have prior creditable service. If so, this date is constructed to include your total years, months and days of prior creditable civilian and military service.
- Full-time employees with fewer than 3 years of service earn 4 hours of annual leave each pay period; those with 3 or more years but less than 15 years earn 6 hours each pay period; and those with 15 or more years earn 8 hours each pay period.
- Your earnings and leave statement or your time and attendance card will

Block 32 - Work Schedule

- Your work schedule is established by your supervisor.
- A full-time employee works on a prearranged scheduled tour of duty that is usually 40 hours per week. A part-time employee has a prearranged scheduled tour of duty that is usually between 16 and 32 hours per week. An intermittent employee has no prearranged scheduled tour of duty and works when needed.
  Full-Time and part-time employees whose appointments are for 90 days or more are usually eligible to earn annual leave; intermittent employees are not.
  Seasonal employees work on an annually recurring bases for periods of less than 12 months each year; they may have a full-time, a part-time, or an intermittent schedule during their work season.
  On-call employees work during periods of heavy workload and are in pay status for at least 6 months of each year; they may have either a full-time or a part-time schedule when they are in pay status.

Block 33 - Part-time Hours Per Biweekly Pay Period

Indicates the number of hours a part-time employee is scheduled to work during a two-week pay period.

Block 34 - Position Occupied

Identifies the employment system under which you are serving -- the Competitive Service, the Excepted Service, or the Senior Executive Service (SES).
The employment system determines your eligibility to move to other jobs in the Federal service, your rights in disciplinary and adverse actions, and your eligibility for reemployment if you have Federal service.

Block 35 - FLSA Category

Exempt employees are not covered by the minimum wage and overtime law (the Fair Labor Standards Act); nonexempt employees are covered.

Block 37 - Bargaining Unit Status

Identifies a bargaining unit to which you belong, whether or not your are actually a member of a labor organization. Code "7777" indicates you are eligible but not in a bargaining unit; code "8888" indicates you are ineligible for inclusion in a bargaining unit.

Block 38 and 39 - Duty Station

Identifies the city, county, and state or the overseas location, where you actually work.

OTHER INFORMATION

- If your appointment entitles you to elect health benefits or life insurance, and you have not been provided materials explaining the programs available and the enrollment forms, contact your personnel specialist.
- Your personnel specialist will also tell you if your position is covered by an agreement between an employee organization (union) and your agency. If you are eligible to and elect to join an employee organization, you can elect to have your dues withheld from your salary.
- If you have questions or need more information about your rights and benefits, ask your supervisor or your personnel office.
- Definitions for any coded data in Blocks 1-24, 27-39 and 45-50 may be found in Federal Personnel Manual Supplement 292-1.

It is your responsibility to read all the information on the front of this notice and tell your personnel office immediately if there is an error in it.

Standard Form 50
Rev. 7/91
U.S. Office of Personnel Management
FPM Supp. 296-33, Subch. 4

NOTIFICATION OF PERSONNEL ACTION

1. Name *(Last, First, Middle)*	2. Social Security Number	3. Date of Birth	4. Effective Date
OPM-5	[redacted]	[redacted]	02/18/2025

FIRST ACTION

5-A. Code	5-B. Nature of Action
570	CONV TO EXC APPT
5-C. Code	**5-D. Legal Authority**
Y7M	SCH C, 213.3391.
5-E. Code	**5-F. Legal Authority**

SECOND ACTION

6-A. Code	6-B. Nature of Action
6-C. Code	**6-D. Legal Authority**
6-E. Code	**6-F. Legal Authority**

7. FROM: Position Title and Number
SENIOR ADVISOR TO THE DIRECTOR FOR INFORMATION TECHNOLOGY
PD: 6A38025

8. Pay Plan	9. Occ. Code	10. Grade or Level	11. Step or Rate	12. Total Salary	13. Pay Basis
GS	0301	15	10	$195,200.00	PA

12A. Basic Pay	12B. Locality Adj.	12C. Adj. Basic Pay	12D. Other Pay
$162,672.00	$32,528.00	$195,200.00	$0

14. Name and Location of Position's Organization
OPM
OFC OF THE DIRECTOR
WASHINGTON DC

15. TO: Position Title and Number
SENIOR ADVISOR TO THE DIRECTOR FOR INFORMATION TECHNOLOGY
PD: 6A38025

16. Pay Plan	17. Occ. Code	18. Grade or Level	19. Step or Rate	20. Total Salary/Award	21. Pay Basis
GS	0301	15	10	$195,200.00	PA

20A. Basic Pay	20B. Locality Adj.	20C. Adj. Basic Pay	20D. Other Pay
$162,672.00	$32,528.00	$195,200.00	$0

22. Name and Location of Position's Organization
OPM
OFC OF THE DIRECTOR
WASHINGTON DC

EMPLOYEE DATA

23. Veterans Preference
1 - None 3 - 10 Point/Disability 5 - 10 Point/Other
2 - 5 Point 4 - 10 Point/Compensable 6 - 10 Point/Compensable/30%
1

24. Tenure
0 - None 2 - Conditional
1 - Permanent 3 - Indefinite
3

25. Agency Use
JS

26. Veterans Pref for RIF
YES [✓ X NO]

27. FEGLI
B0 [redacted]

28. Annuitant Indicator
9 NOT APPLICABLE

29. Pay Rate Determinant
7

30. Retirement Plan
KF [redacted]

31. Service Comp. Date (Leave)
01/20/2025

32. Work Schedule
F FULL TIME

33. Part-Time Hours Per Biweekly Pay Period

POSITION DATA

34. Position Occupied
1 - Competitive Service 3 - SES General
2 - Excepted Service 4 - SES Career
2

35. FLSA Category
E - Exempt
N - Nonexempt
E

36. Appropriation Code
41AA0

37. Bargaining Unit Status
8888

38. Duty Station Code
11-0010-001

39. Duty Station *(City - County - State or Overseas Location)*
WASHINGTON DISTRICT OF COLUMBIA DC

40. AGENCY DATA	41.	42.	43.	44.
10001		0000	33.94	CRITICAL-SENSITIVE (CS)/HIGH R

45. Remarks
POSITION IS AT THE FULL PERFORMANCE LEVEL OR BAND.
OPM FORM 1019 DATED 02-18-2025.

46. Employing Department or Agency
OPM

47. Agency Code	48. Personnel Office ID	49. Approval Date
OM00	1000	02/20/2025

50. Signature/Authentication and Title of Approving Official
ELECTRONICALLY SIGNED BY:
CARMEN GARCIA-WHITESIDE
CHIEF HUMAN CAPITAL OFFICER AND DIRECTOR OF OPM HR

5-Part **2 - OPF Copy - Long-Term Record -- DO NOT DESTROY**

Editions Prior to 7/91 Are Not Usable After 6/30/93
NSN 7540-01-333-6236

NOTICE TO EMPLOYEE

This is your copy of the official notice of a personnel action. Keep it with your records because it could be used to make employment, pay, and qualifications decisions about you in the future.

The Action

- Blocks 5-B and 6-B describe the personnel action(s) that occurred.
- Blocks 15-22 show the position and organization to which you are assigned.

Pay

- When the personnel action is an award or bonus, block 20 shows the amount of that one-time cash payment. When the action is not an award or bonus, block 12 shows your former total annual salary, and block 20 shows your new total annual salary (block 20C plus 20D). The amounts in blocks 12 and 20 do not include any one-time cash payments (such as performance awards and recruitment or relocation bonuses) or payments that may vary from one pay period to the next (such as overtime pay), or other forms of premium pay.
- Block 20A is the scheduled amount for your grade and step, including any special salary rate you receive. It does not include any locality-based pay. This rate of pay serves as the basis for determining your rate of pay upon promotion, change to a lower grade, or reassignment, and is used for pay retention purposes.
- Block 20B is the annual dollar amount of your interim Geographic Adjustment or, beginning in 1994, your locality-based comparability payment.
- Block 20C is your Adjusted Basic Pay, the total of blocks 20A and 20B. It serves as the basis for computing your retirement benefits, life insurance, premium pay, and severance pay.
- Block 20D is the total dollar amount of any Retention Allowances, Supervisory Differentials, and Staffing Differentials that are listed in the remarks block. These payments are made in the same manner as basic pay, but are not a part of basic pay for any purpose.

Block 24 - Tenure

- Identifies the nature of your appointment and is used to determine your rights during a reduction in force (RIF). Tenure groups are explained in more detail in subchapter 26 of FPM Supplement 296-33 and RIF is explained in FPM Supplement 351-1; both should be available for review in your personnel office.

Block 26 - Veterans Preference to RIF

- Indicates whether you have preference for reduction-in-force purposes.

Block 30 - Retirement Plan

- **FICA** - Social Security System
- **CS** - Civil Service Retirement System
- **CS-Spec** - Civil Service Retirement System for law enforcement and firefighter personnel
- **FS** - Foreign Service Retirement and Disability System
- **FERS** - Federal Employees' Retirement System
- **FERS-Reserve Tech** - Federal Employees' Retirement System for National Guard Reserve Technicians
- **FERS-ATC** - Federal Employees' Retirement System for Air Traffic Controllers
- **FERS-Spec** - Federal Employees' Retirement System for law enforcement and firefighter personnel
- **FSPS** - Foreign Service Pension System

Block 31 - Service computation Date (Leave)

- Shows when your Federal service began unless you have prior creditable service. If so, this date is constructed to include your total years, months and days of prior creditable civilian and military service.
- Full-time employees with fewer than 3 years of service earn 4 hours of annual leave each pay period; those with 3 or more years but less than 15 years earn 6 hours each pay period; and those with 15 or more years earn 8 hours each pay period.
- Your earnings and leave statement or your time and attendance card will

Block 32 - Work Schedule

- Your work schedule is established by your supervisor.
- A full-time employee works on a prearranged scheduled tour of duty that is usually 40 hours per week. A part-time employee has a prearranged scheduled tour of duty that is usually between 16 and 32 hours per week. An intermittent employee has no prearranged scheduled tour of duty and works when needed.
  Full-Time and part-time employees whose appointments are for 90 days or more are usually eligible to earn annual leave; intermittent employees are not. Seasonal employees work on an annually recurring bases for periods of less than 12 months each year; they may have a full-time, a part-time, or an intermittent schedule during their work season.
  On-call employees work during periods of heavy workload and are in pay status for at least 6 months of each year; they may have either a full-time or a part-time schedule when they are in pay status.

Block 33 - Part-time Hours Per Biweekly Pay Period

Indicates the number of hours a part-time employee is scheduled to work during a two-week pay period.

Block 34 - Position Occupied

Identifies the employment system under which you are serving -- the Competitive Service, the Excepted Service, or the Senior Executive Service (SES).
The employment system determines your eligibility to move to other jobs in the Federal service, your rights in disciplinary and adverse actions, and your eligibility for reemployment if you have Federal service.

Block 35 - FLSA Category

Exempt employees are not covered by the minimum wage and overtime law (the Fair Labor Standards Act); nonexempt employees are covered.

Block 37 - Bargaining Unit Status

Identifies a bargaining unit to which you belong, whether or not your are actually a member of a labor organization. Code "7777" indicates you are eligible but not in a bargaining unit; code "8888" indicates you are ineligible for inclusion in a bargaining unit.

Block 38 and 39 - Duty Station

Identifies the city, county, and state or the overseas location, where you actually work.

OTHER INFORMATION

- If your appointment entitles you to elect health benefits or life insurance, and you have not been provided materials explaining the programs available and the enrollment forms, contact your personnel specialist.
- Your personnel specialist will also tell you if your position is covered by an agreement between an employee organization (union) and your agency. If you are eligible to and elect to join an employee organization, you can elect to have your dues withheld from your salary.
- If you have questions or need more information about your rights and benefits, ask your supervisor or your personnel office.
- Definitions for any coded data in Blocks 1-24, 27-39 and 45-50 may be found in Federal Personnel Manual Supplement 292-1.

It is your responsibility to read all the information on the front of this notice and tell your personnel office immediately if there is an error in it.

Standard Form 50
Rev. 7/91
U.S. Office of Personnel Management
FPM Supp. 296-33, Subch. 4

NOTIFICATION OF PERSONNEL ACTION

1. Name (Last, First, Middle) OPM-6	2. Social Security Number [redacted]	3. Date of Birth [redacted]	4. Effective Date 01/24/2025

FIRST ACTION

5-A. Code 171	5-B. Nature of Action EXC APPT NTE 07/22/2025
5-C. Code H2L	5-D. Legal Authority REG 304.103.
5-E. Code	5-F. Legal Authority

SECOND ACTION

6-A. Code	6-B. Nature of Action
6-C. Code	6-D. Legal Authority
6-E. Code	6-F. Legal Authority

7. FROM: Position Title and Number

8. Pay Plan	9. Occ. Code	10. Grade or Level	11. Step or Rate	12. Total Salary	13. Pay Basis

12A. Basic Pay	12B. Locality Adj.	12C. Adj. Basic Pay	12D. Other Pay

14. Name and Location of Position's Organization

15. TO: Position Title and Number
EXPERT
PD: 6A39738

16. Pay Plan	17. Occ. Code	18. Grade or Level	19. Step or Rate	20. Total Salary/Award	21. Pay Basis
ED	0301	00	00	$0	WC

20A. Basic Pay	20B. Locality Adj.	20C. Adj. Basic Pay	20D. Other Pay
$0	$0	$0	$0

22. Name and Location of Position's Organization
OPM
OFC OF THE DIRECTOR

WASHINGTON DC

EMPLOYEE DATA

23. Veterans Preference: 1 (1 - None; 2 - 5-Point; 3 - 10-Point/Disability; 4 - 10-Point/Compensable; 5 - 10-Point/Other; 6 - 10-Point/Compensable/30%)

24. Tenure: 0 (0 - None; 1 - Permanent; 2 - Conditional; 3 - Indefinite)

25. Agency Use: TG

26. Veterans Preference for RIF: YES [✓ X NO]

27. FEGLI: A0 [redacted]

28. Annuitant Indicator: 9 NOT APPLICABLE

29. Pay Rate Determinant: 0

30. Retirement Plan: 4 [redacted]

31. Service Comp. Date (Leave): 01/24/2025

32. Work Schedule: F FULL TIME

33. Part-Time Hours Per Biweekly Pay Period:

POSITION DATA

34. Position Occupied: 2 (1 - Competitive Service; 2 - Excepted Service; 3 - SES General; 4 - SES Career Reserved)

35. FLSA Category: E (E - Exempt; N - Nonexempt)

36. Appropriation Code: 41AA0

37. Bargaining Unit Status: 8888

38. Duty Station Code: 11-0010-001

39. Duty Station (City - County - State or Overseas Location): WASHINGTON DISTRICT OF COLUMBIA DC

40. Agency Data	41.	42.	43.	44.
10001		0000	33.94	CRITICAL-SENSITIVE (CS)/HIGH R

45. Remarks
```
APPOINTMENT AFFIDAVIT EXECUTED 01-24-2025
REASON FOR TEMPORARY APPOINTMENT:   TO PROVIDE A HIGH LEVEL OF EXPERTISE RELATIVE TO ISSUES WHICH HAVE A
 SIGNIFICANT IMPACT ON THE FORMULATION OF AGENCY GOALS AND OBJECTIVES TO THE OPM DIRECTOR.
CREDITABLE MILITARY SERVICE: NONE
PREVIOUS RETIREMENT COVERAGE: NEVER COVERED
```

46. Employing Department or Agency: OPM

47. Agency Code	48. Personnel Office ID	49. Approval Date
OM00	1000	01/30/2025

50. Signature/Authentication and Title of Approving Official
ELECTRONICALLY SIGNED BY:
CARMEN GARCIA-WHITESIDE
CHIEF HUMAN CAPITAL OFFICER AND DIRECTOR OF OPM HR

5-Part 50-316

2 - OPF Copy - Long-Term Record - DO NOT DESTROY

Editions Prior to 7/91 Are Not Usable After 6/30/93
NSN 7540-01-333-6238

APPOINTMENT AFFIDAVITS

Expert	01/24/2025
(Position to which Appointed)	*(Date Appointed)*

Office of Personnel Managemer	Office of the Director	Washington, D.C.
(Department or Agency)	*(Bureau or Division)*	*(Place of Employment)*

I, **OPM-6** , do solemnly swear (or affirm) that--

A. OATH OF OFFICE

I will support and defend the Constitution of the United States against all enemies, foreign and domestic; that I will bear true faith and allegiance to the same; that I take this obligation freely, without any mental reservation or purpose of evasion; and that I will well and faithfully discharge the duties of the office on which I am about to enter. So help me God.

B. AFFIDAVIT AS TO STRIKING AGAINST THE FEDERAL GOVERNMENT

I am not participating in any strike against the Government of the United States or any agency thereof, and I will not so participate while an employee of the Government of the United States or any agency thereof.

C. AFFIDAVIT AS TO THE PURCHASE AND SALE OF OFFICE

I have not, nor has anyone acting in my behalf, given, transferred, promised or paid any consideration for or in expectation or hope of receiving assistance in securing this appointment.

OPM-6
(Signature of Appointee)

Subscribed and sworn (or affirmed) before me this 24 day of JANUARY , 2025

at WASHINGTON (City) D.C (State)

[illegible]
(Signature of Officer)

(SEAL)

Commission expires ____________
(If by a Notary Public, the date of his/her Commission should be shown)

SUPERVISORY HR SPECIALIST
(Title)

Note - If the appointee objects to the form of the oath on religious grounds, certain modifications may be permitted pursuant to the Religious Freedom Restoration Act. Please contact your agency's legal counsel for advice.

From: Hogan, Greg
To: Foster, Ozie L.; Price, MC
Cc: Ezell, Charles E.
Subject: Re: Getting DoGE Engineers access
Date: Sunday, February 16, 2025 6:52:09 PM

Thank you, that was the info I was looking for.

Greg

From: Foster, Ozie L. <[redacted]@opm.gov>
Sent: Sunday, February 16, 2025 6:39 PM
To: Hogan, Greg <[redacted]@opm.gov>; Price, MC <[redacted]@opm.gov>
Cc: Ezell, Charles E. <[redacted]@opm.gov>
Subject: Re: Getting DoGE Engineers access

You're welcome, Greg. Your account was never created. If you do need an account we can get you setup Tuesday AM.

The only 3 accounts created were for **OPM-4**, **OPM-2**, and **OPM-6** for eOPF and EHRI.

Danielle's file below was updated with user names, system names and dates. You will see where their accounts were added and removed + many other updates associated with OPM Data systems.

Account Creation Audit.xlsx

Thank you,

Ozie Foster
Supervisory IT Specialist
U.S. Office of Personnel Management
OCIO, Federal Information Technology Business Solutions
(478) [redacted]
[redacted]@opm.gov
OPM.gov

Follow us on LinkedIn | Twitter | YouTube

From: Hogan, Greg <[redacted]@opm.gov>
Sent: Sunday, February 16, 2025 5:43 PM
To: Foster, Ozie L. <[redacted]@opm.gov>; Price, MC <[redacted]@opm.gov>
Cc: Ezell, Charles E. <[redacted]@opm.gov>
Subject: Re: Getting DoGE Engineers access

Thank you for the quick response!

Can you give me the list of people who did have access and we revoked their access?

Also, can you tell me if I have access?

Greg

From: Foster, Ozie L. <[redacted]@opm.gov>
Sent: Sunday, February 16, 2025 4:48 PM
To: Hogan, Greg <[redacted]@opm.gov>; Price, MC [redacted]@opm.gov>
Cc: Ezell, Charles E. [redacted]@opm.gov>
Subject: Re: Getting DoGE Engineers access

Yes. All access is disabled/removed, verified users never logged in for EHRI and eOPF.

Thank you,

Ozie Foster
Supervisory IT Specialist
U.S. Office of Personnel Management
OCIO, Federal Information Technology Business Solutions
(478) [redacted]
[redacted]@opm.gov
OPM.gov

Follow us on LinkedIn | Twitter | YouTube

From: Hogan, Greg <[redacted]@opm.gov>
Sent: Sunday, February 16, 2025 4:26:22 PM
To: Price, MC <[redacted]@opm.gov>; Foster, Ozie L. [redacted]@opm.gov>
Cc: Ezell, Charles E. [redacted]@opm.gov>
Subject: Re: Getting DoGE Engineers access

Did we follow up on OPM-5, OPM-3, and OPM-4? Sorry if I missed it.

Greg

From: Price, MC <[redacted]@opm.gov>
Sent: Thursday, February 6, 2025 10:28 PM
To: Foster, Ozie L. <[redacted]@opm.gov>

Cc: Hogan, Greg <[redacted]@opm.gov>; Ezell, Charles E. <[redacted]@opm.gov>
Subject: Re: Getting DoGE Engineers access

Thx Ozie!!

On Feb 6, 2025, at 10:04 PM, Foster, Ozie L. [redacted]@opm.gov> wrote:

Good evening, everyone

OPM-6 and OPM-2 accounts have been disabled for both EHRI DW [on prem] and eOPF [on prem Oracle & Azure SQL]. Also OPS verification that accounts were never used.

I will verify account status for OPM-5, OPM-3, and OPM-4 in the AM but I'm sure it's the same of unused.

Thank you,

Ozie Foster
Supervisory IT Specialist
U.S. Office of Personnel Management
OCIO, Business Applications Services
(478)[redacted]
[redacted]@opm.gov
OPM.gov

<Image.png>

Follow us on LinkedIn | Twitter | YouTube

From: Price, MC [redacted]@opm.gov>
Sent: Thursday, February 6, 2025 7:44 PM
To: Hogan, Greg [redacted]@opm.gov>
Cc: Ezell, Charles E. <[redacted]@opm.gov>; Foster, Ozie L. [redacted]@opm.gov>
Subject: Re: Getting DoGE Engineers access

+Ozie

Greg,

OPM-6 and OPM-2 had access to eOPF/eHRI but never logged in. OPM-4 never completed the process to get access.

Ozie will get them removed tomorrow morning.

Thx, MC

On Feb 6, 2025, at 6:10 PM, Hogan, Greg <[redacted]@opm.gov> wrote:

MC:

I will get back to you tomorrow on your list below. In the mean time, we have never needed access to ERHI/eOPF so if any access was granted there it can be removed immediately, and your DBAs can have their access back immediately, too.

Greg

From: Price, MC <[redacted]@opm.gov>
Sent: Thursday, February 6, 2025 5:33 PM
To: Hogan, Greg <[redacted]@opm.gov>
Cc: Ezell, Charles E. [redacted]@opm.gov>
Subject: RE: Getting DoGE Engineers access

I will check, however, I believe the folks listed below have full Production access to OPM.gov, USAJOBS, USA Staffing and USA Performance, to our Azure landing zones, and to Akamai portal.

Do you want to remove them? And if so, do you want to return our OCIO folks to their original permissions?

MC

From: Hogan, Greg [redacted]@opm.gov>
Sent: Thursday, February 6, 2025 5:27 PM
To: Price, MC [redacted]@opm.gov>
Cc: Ezell, Charles E. <[redacted]@opm.gov>
Subject: Re: Getting DoGE Engineers access

Can someone share with me what access is still set up that was in response to the below email chain?

Based on the below email chain, it looks like this is the list of people that may have been granted access to certain systems:

OPM-6 @opm.gov
OPM-2 @opm.gov
OPM-4 @opm.gov
OPM-5 @opm.gov
OPM-3 @opm.gov

I want to start unwinding peoples access if it is currently unnecessary.

Greg

From: Ezell, Charles E. <[redacted]@opm.gov>
Sent: Monday, January 27, 2025 5:29 PM
To: ScalesOLD, Amanda <[redacted]@opm.gov>; OPM-6 [redacted]@opm.gov>; Hogan, Greg <[redacted]@opm.gov>; OPM-7 OPM-6, OPM-7 [redacted]@opm.gov>
Subject: Fw: Getting DoGE Engineers access

Apologies I should've copied you all on this when I sent it.

.ce

Chuck Ezell
Acting Director

U.S. Office of Personnel Management
o: (478)[redacted]
c: (478)[redacted]
[redacted]@OPM.gov
OPM.gov

From: Ezell, Charles E. <[redacted]@opm.gov>
Sent: Monday, January 27, 2025 5:03 PM
To: Price, MC <[redacted]@opm.gov>
Subject: Re: Getting DoGE Engineers access

Yep, I understand. They won't have a lot of time to go through a lot of presentations on what the systems are and what the program officers feel about the programs, etc. You understand.... Bu it there is an architecture level engineering perspective that could be shared that might be helpful if it could be done at some point.

OPM-6 @opm.gov
OPM-2 @opm.gov
OPM-4 @opm.gov

.ce

Chuck Ezell
Acting Director

U.S. Office of Personnel Management
o: (478) [redacted]
c: (478) [redacted]
[redacted]@OPM.gov
OPM.gov

From: Price, MC <[redacted]@opm.gov>
Sent: Monday, January 27, 2025 4:32:04 PM
To: Ezell, Charles E. [redacted]@opm.gov>
Subject: RE: Getting DoGE Engineers access

Sure, just send me a list of names and we'll give them access and hook them up with the folks that can give them the deep dive/documentation on the Apps.

I'm assuming these engineers have GFE/PIVs or will get them soon?

One note, some of the HI systems we simply host and do not have the dev access….those devs live in HI.

MC

From: Ezell, Charles E. <[redacted]@opm.gov>
Sent: Monday, January 27, 2025 4:20 PM
To: Price, MC <[redacted]@opm.gov>
Subject: Getting DoGE Engineers access

MC,

We are rapidly ramping up some engineers here. To accomplish this goal, these engineers need the following items urgently, starting with a short list of all the systems OPM operates and manages.

Right now we don't have immediate plans to change anything but if we need to we might need to move quickly.

For each computer system, (whewe need:

• Code read and write permissions
• Deploy ability Octopus deploy
• Monitoring dashboards (e.g. displaying success rates, volume of traffic)
• Documentation (e.g. test and deploy instructions, system diagrams)
• The on-call rotation for the system
• Names of all engineers deeply familiar with the system
• Names of all product/project managers deeply familiar with the system
• Ability to access the system as a regular user (e.g. hiring manager and onboarding user for USA Staffing)
• Ability to access the system as an admin user
Prioritize USA Staffing, USAJOBS, and EHRI.

Again we don't have any immediate plans for new engineers to make direct changes to any of these systems.

I'll get you the list of Engineers but I think **OPM-5** and **OPM-3** have already been setup with some access.

Thank you

.ce

Chuck Ezell
Acting Director

U.S. Office of Personnel Management
o: (478) [redacted]
c: (478) [redacted]
[redacted]@OPM.gov
OPM.gov

From: Pinto, Delon G. F.
To: Rowell, Danielle R
Cc: Hogan, Greg; Saunders, James L; Muetzel, James
Subject: RE: Internal User Access Audit
Date: Tuesday, February 18, 2025 4:00:37 PM
Attachments: image002.png
image003.png

Good afternoon,

I'm confirming that FLTCIP and FSAFEDS do not have internal OPM user accounts. Let me know if you need anything else.

Best,
Delon

From: Rowell, Danielle R <[redacted]@opm.gov>
Sent: Tuesday, February 18, 2025 1:01 PM
To: CISO [redacted]@opm.gov>
Cc: Hogan, Greg <[redacted]@opm.gov>; Saunders, James L [redacted]@opm.gov>; OCIO-Leadership [redacted]@opm.gov>
Subject: RE: Internal User Access Audit

Good Afternoon,

Thank you for responding to the initial audit call. In addition to the original ask, we're asking that you please provide the Cybersecurity Division with **evidence of the system account approvals** for all internal OPM user accounts created since 1/20/2025 until 2/12/25 (Please use list of already identified users). As the System Owner responsible for approving OPM information system access, please provide the formal approval artifact for all internal OPM accounts created during this timeframe." **All responses are due by 2/20/2025.**

Example Artifacts:

1. Email request from user and approval.
2. Email request to helpdesk with approval from supervisor.
3. Azure access packages approvals.
4. Other.

Account Creation Artifacts

Thanks!

Danielle Rowell
OPM.gov

Follow us on LinkedIn | Twitter | YouTube

From: Rowell, Danielle R
Sent: Wednesday, February 12, 2025 4:27 PM
To: CISO [redacted]@opm.gov>
Cc: Hogan, Greg <[redacted]@opm.gov>; Saunders, James L <[redacted]@opm.gov>; OCIO-Leadership [redacted]@opm.gov>
Subject: Internal User Access Audit
Importance: High

Good Evening,

As requested by the OPM CIO, the Cybersecurity Division is conducting a review of **all internal OPM user accounts** created between 1/20/2025 and 2/12/25 As the System Owner responsible for approving access to an OPM information system, please provide the following information. **All responses are due by 2/17/25**.

Account Creation Audit

- Employee Name
- Account Username
- System Name
- Date Created

Please provide questions to [redacted]@opm.gov.

Thanks!

Danielle Rowell
Acting Chief Information Security Officer, Cybersecurity Division

U.S. Office of Personnel Management
Office of the Chief Information Officer
c: 202-[redacted]
o: 202-[redacted]
[redacted]@opm.gov
OPM.gov

Follow us on LinkedIn | Twitter | YouTube

Isaiah 41:10

will occur with the receipt of both benefits.

Analysis

Agency: Office of Personnel Management, Retirement Services.

Title: We Need Important Information About Your Eligibility for Social Security Disability Benefits.

OMB Number: 3206–0216.

Frequency: On occasion.

Affected Public: Individuals or Households.

Number of Respondents: 4,300.

Estimated Time per Respondent: 5 minutes.

Total Burden Hours: 358.

Office of Personnel Management.

Kayyonne Marston,

Federal Register Liaison.

[FR Doc. 2023–17640 Filed 8–16–23; 8:45 am]

BILLING CODE 6325–38–P

OFFICE OF PERSONNEL MANAGEMENT

[Docket ID: OPM–2023–0024]

Privacy Act of 1974; System of Records

AGENCY: Office of Personnel Management.

ACTION: Notice of a modified system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Office of Personnel Management (OPM) proposes to modify an OPM system of records titled, "OPM/GOVT–1 General Personnel Records" System of Records. The records in this system of records are maintained by OPM and employing agencies in accordance with OPM regulations and instructions. OPM proposes to modify this system of records by revising Routine Uses "s" and "hh".

DATES: Submit comments on or before September 18, 2023. The modified routine uses will be effective on September 21, 2023.

ADDRESSES: You may submit written comments by one of the following methods:

• *Federal Rulemaking Portal: https://www.regulations.gov.*

All submissions received must include the agency name and docket number for this **Federal Register** document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the internet at *https://www.regulations.gov* as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Marc Flaster, Senior Agency Official for Privacy (Acting), Office of Personnel Management at *privacy@opm.gov.*

SUPPLEMENTARY INFORMATION: In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Office of Personnel Management ("OPM"), proposes to make certain modifications to the "OPM/GOVT–1 General Personnel Records" system of records pending a comprehensive review and update at a later date. Specifically, OPM proposes to revise Routine Use "s" to specify that OPM may disclose records from this system of records to other Federal entities for the purpose of conducting research and statistical analysis for government-wide evaluation and reporting about the Federal workforce. In its current form, Routine Use "s" only permits internal use of the records for such purposes.

Routine Use "s" currently reads as follows:

s. By the agency maintaining the records or by the OPM to locate individuals for personnel research or survey response, and in the production of summary descriptive statistics and analytical studies in support of the function for which the records are collected and maintained, or for related workforce studies. While published statistics and studies do not contain individual identifiers, in some instances, the selection of elements of data included in the study may be structured in such a way as to make the data individually identifiable by inference.

OPM proposes to revise Routine Use "s" to read as follows:

s. To disclose to another Federal agency, by the agency maintaining the records or by OPM, for research or analytical purposes, including to locate individuals for personnel research or survey response, to produce summary descriptive statistics, or to conduct analytical studies in support of the function for which the records are collected and maintained, or for related workforce studies; provided that the disclosure is made pursuant to a written agreement that clearly outlines the relevant authorities, limits the disclosure only to those records that are necessary for a clearly documented purpose, and limits the use of the records for that purpose.

OPM also proposes to revise Routine Use "hh" to clarify that the records in this system of records may be disclosed in the context of an appropriate computer matching program. The current language of this Routine Use does not track the definition of "matching program" in the Privacy Act and the revised language is intended to correct that and permit disclosure in the context of any approved matching program that meets the definition in the Act.

Routine Use "hh" currently reads as follows:

hh. To disclose relevant information with personal identifiers of Federal civilian employees whose records are contained in the EHRI to authorized Federal agencies and non-Federal entities for use in computer matching. The matches will be performed to help eliminate waste, fraud, and abuse in Governmental programs; to help identify individuals who are potentially in violation of civil or criminal law or regulation; and to collect debts and overpayments owed to Federal, State, or local governments and their components. The information disclosed may include, but is not limited to, the name, social security number, date of birth, sex, annualized salary rate, service computation date of basic active service, veteran's preference, retirement status, occupational series, health plan code, position occupied, work schedule (full time, part time, or intermittent), agency identifier, geographic location (duty station location), standard metropolitan service area, special program identifier, and submitting office number of Federal employees.

OPM proposed to revise Routine Use "hh" to read as follows:

hh. To other Federal agencies, such as the Social Security Administration, the Department of Education, and the Department of Health and Human Services, and to non-Federal entities, relevant information with personal identifiers of Federal civilian employees whose records are contained in the EHRI to authorized Federal agencies and non-Federal entities for use in a computer matching program, as defined in 5 U.S.C. 552a(a)(8), to help eliminate waste, fraud, and abuse in Governmental programs; to help identify individuals who are potentially in violation of civil or criminal law or regulation; to collect debts and overpayments owed to Federal, State, or local governments and their components; and to identify individuals as Federal civilian employees when relevant to their receiving a benefit from the matching partner.

In addition to revising the above-referenced Routine Uses, OPM also proposes to make certain administrative adjustments to the SORN to update the System Manager to reflect organizational changes at OPM and to update the description of the System Location for accuracy.

OPM has provided a report of this modified system of records to the Committee on Oversight and Government Reform of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Office of Management and Budget (OMB), pursuant to 5 U.S.C. 552a(r) and OMB Circular A–108, ''Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act,'' dated December 23, 2016. This modified system will be included in OPM's inventory of records systems.

Office of Personnel Management.

Kayyonne Marston,

Federal Register Liaison.

SYSTEM NAME AND NUMBER:

General Personnel Records, OPM/GOVT–1.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Records on current Federal employees are located within the employing agency. Records maintained in paper may also be located at OPM or with personnel officers, or at other designated offices of local installations of the department or agency that employs the individual. When agencies determine that duplicates of these records need to be located in a second office, *e.g.,* an administrative office closer to where the employee actually works, such copies are covered by this system of records. Some agencies have employed the electronic Official Personnel Folder (eOPF) information technology system to store their records electronically. Although stored in eOPF, agencies are still responsible for the maintenance of their records. In addition, certain data elements from the eOPF are collected and maintained in OPM's Enterprise Human Resource Integration (EHRI) system.

Former Federal employees' paper Official Personnel Folders (OPFs) are located at the National Personnel Records Center, National Archives and Records Administration, in Valmeyer, Illinois. Former Federal employees' electronic Official Personnel Folders (eOPF) are located in the eOPF system at OPM.

Note 1—The records in this system are records of the OPM and must be provided to those OPM employees who have an official need or use for those records. Therefore, if an employing agency is asked by an OPM employee to access the records within this system, such a request must be honored.

SYSTEM MANAGER(S):

a. Executive Director, Human Capital Data Management and Modernization, U.S. Office of Personnel Management, 1900 E Street NW, Washington, DC 20415; Associate Director, Employee Services, U.S. Office of Personnel Management, 1900 E Street NW, Washington, DC 20415.

b. For current Federal employees, OPM has delegated to the employing agency the Privacy Act responsibilities concerning access, amendment, and disclosure of the records within this system notice.

* * * * *

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

* * * * *

s. To disclose to another Federal agency, by the agency maintaining the records or by OPM, for research or analytical purposes, including to locate individuals for personnel research or survey response, to produce summary descriptive statistics, or to conduct analytical studies in support of the function for which the records are collected and maintained, or for related workforce studies; provided that the disclosure is made pursuant to a written agreement that clearly outlines the relevant authorities, limits the disclosure only to those records that are necessary for a clearly documented purpose, and limits the use of the records for that purpose.

* * * * *

hh. To other Federal agencies, such as the Social Security Administration, the Department of Education, and the Department of Health and Human Services, and to non-Federal entities, relevant information with personal identifiers of Federal civilian employees whose records are contained in the EHRI to authorized Federal agencies and non-Federal entities for use in a computer matching program, as defined in 5 U.S.C. 552a(a)(8), to help eliminate waste, fraud, and abuse in Governmental programs; to help identify individuals who are potentially in violation of civil or criminal law or regulation; to collect debts and overpayments owed to Federal, State, or local governments and their components; and to identify individuals as Federal civilian employees when relevant to their receiving a benefit from the matching partner.

* * * * *

HISTORY:

OPM/GOVT–1, ''General Personnel Records'', 77 FR 73694 (December 11, 2012), 80 FR 74815 (November 30, 2015), 76 FR 32997 (June 7, 2011), 71 FR 35342 (June 19, 2006), 65 FR 24732 (April 27, 2000), and 61 FR 36919 (July 15, 1996).

[FR Doc. 2023–17651 Filed 8–16–23; 8:45 am]

BILLING CODE 6325–67–P

POSTAL REGULATORY COMMISSION

[Docket Nos. MC2023–220 and CP2023–224; MC2023–221 and CP2023–225; MC2023–223 and CP2023–226; MC2023–224 and CP2023–227]

New Postal Products

AGENCY: Postal Regulatory Commission.

ACTION: Notice.

SUMMARY: The Commission is noticing a recent Postal Service filing for the Commission's consideration concerning a negotiated service agreement. This notice informs the public of the filing, invites public comment, and takes other administrative steps.

DATES: *Comments are due:* August 21, 2023.

ADDRESSES: Submit comments electronically via the Commission's Filing Online system at *http://www.prc.gov.* Those who cannot submit comments electronically should contact the person identified in the **FOR FURTHER INFORMATION CONTACT** section by telephone for advice on filing alternatives.

FOR FURTHER INFORMATION CONTACT: David A. Trissell, General Counsel, at 202–789–6820.

SUPPLEMENTARY INFORMATION:

Table of Contents

I. Introduction
II. Docketed Proceeding(s)

I. Introduction

The Commission gives notice that the Postal Service filed request(s) for the Commission to consider matters related to negotiated service agreement(s). The request(s) may propose the addition or removal of a negotiated service agreement from the Market Dominant or the Competitive product list, or the modification of an existing product currently appearing on the Market Dominant or the Competitive product list.

Section II identifies the docket number(s) associated with each Postal Service request, the title of each Postal Service request, the request's acceptance date, and the authority cited by the

For the Nuclear Regulatory Commission.

Michele G. Evans,

Director, Division of Operating Reactor Licensing, Office of Nuclear Reactor Regulation.

[FR Doc. 2012–29612 Filed 12–10–12; 8:45 am]

BILLING CODE 7590–01–P

NUCLEAR REGULATORY COMMISSION

Sunshine Federal Register Notice

AGENCY HOLDING THE MEETINGS: Nuclear Regulatory Commission [NRC–2012–0002].

DATES: Weeks of December 10, 17, 24, 31, 2012, January 7, 14, 2013.

PLACE: Commissioners' Conference Room, 11555 Rockville Pike, Rockville, Maryland.

STATUS: Public and Closed.

Week of December 10, 2012

There are no meetings scheduled for the week of December 10, 2012.

Week of December 17, 2012—Tentative

There are no meetings scheduled for the week of December 17, 2012.

Week of December 24, 2012—Tentative

There are no meetings scheduled for the week of December 24, 2012.

Week of December 31, 2012—Tentative

There are no meetings scheduled for the week of December 31, 2012.

Week of January 7, 2013—Tentative

Tuesday, January 8, 2013

9:00 a.m. Briefing on Fort Calhoun (Public Meeting). (Contact: Michael Hay, 817–200–1527).

This meeting will be webcast live at the Web address—*www.nrc.gov.*

Week of January 14, 2013—Tentative

There are no meetings scheduled for the week of January 14, 2013.

* * * * *

* The schedule for Commission meetings is subject to change on short notice. To verify the status of meetings, call (recording)—301–415–1292. Contact person for more information: Rochelle Bavol, 301–415–1651.

* * * * *

The NRC Commission Meeting Schedule can be found on the Internet at: *http://www.nrc.gov/public-involve/public-meetings/schedule.html.*

* * * * *

The NRC provides reasonable accommodation to individuals with disabilities where appropriate. If you need a reasonable accommodation to participate in these public meetings, or need this meeting notice or the transcript or other information from the public meetings in another format (e.g. braille, large print), please notify Bill Dosch, Chief, Work Life and Benefits Branch, at 301–415–6200, TDD: 301–415–2100, or by email at *william.dosch@nrc.gov.* Determinations on requests for reasonable accommodation will be made on a case-by-case basis.

* * * * *

This notice is distributed electronically to subscribers. If you no longer wish to receive it, or would like to be added to the distribution, please contact the Office of the Secretary, Washington, DC 20555 (301–415–1969), or send an email to *darlene.wright@nrc.gov.*

Dated: December 6, 2012.

Rochelle C. Bavol,

Policy Coordinator, Office of the Secretary.

[FR Doc. 2012–29954 Filed 12–7–12; 4:15 pm]

BILLING CODE 7590–01–P

OFFICE OF PERSONNEL MANAGEMENT

Privacy Act of 1974: Update Existing System of Records

AGENCY: U.S. Office of Personnel Management.

ACTION: Update OPM/GOVT–1, General Personnel Records.

SUMMARY: The U.S. Office of Personnel Management (OPM) proposes to update OPM/GOVT–1, General Personnel Records, System of Records. This action is necessary to meet the requirements of the Privacy Act to publish in the **Federal Register** notice of the existence and character of records maintained by the agency (5 U.S.C. 552a(e)(4)) and (11).

DATES: This action will be effective without further notice on January 10, 2013 unless comments are received that would result in a contrary determination.

ADDRESSES: Send written comments to the U.S. Office of Personnel Management, Manager, OCIO/RM, 1900 E Street NW., Washington, DC 20415.

FOR FURTHER INFORMATION CONTACT: U.S. Office of Personnel Management, Manager, OCIO/RM, 1900 E Street NW., Washington, DC 20415.

SUPPLEMENTARY INFORMATION: The OPM system of record notice subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended, has been published in the **Federal Register.** The proposed changes include the following: (1) Adding *a reference to* OPM's "Guide to Data Standards" to the "Categories of Records in the System," (2) adding Enterprise Human Resource Integration (EHRI) to Categories of Records in the System (g), (3) shortening existing Note "8,", (4) adding routine use "qq" To disclose foreign language proficiencies to Federal agencies in support of the National Preparedness Goal and the Presidential Policy Directive 8 (PPD–8), and (5) adding routine use "rr" To disclose information to the Centers for Medicare and Medicaid (CMS) to assist in determining whether individuals are eligible for programs under the Patient Protection and Affordable Care Act (PPACA).

U.S. Office of Personnel Management.

John Berry,

Director.

OPM/GOVT–1

SYSTEM NAME:

General Personnel Records.

SYSTEM LOCATION:

Records on current Federal employees are located within the employing agency.

Records maintained in paper may also be located at OPM or with personnel officers, or at other designated offices of local installations of the department or agency that employs the individual. When agencies determine that duplicates of these records need to be located in a second office, e.g., an administrative office closer to where the employee actually works, such copies are covered by this system. Some agencies have employed the Enterprise Human Resource Integration (EHRI) data system to store their records electronically. Although stored in EHRI, agencies are still responsible for the maintenance of their records.

Former Federal employees' paper Official Personnel Folders (OPFs) are located at the National Personnel Records Center, National Archives and Records Administration (NARA), 111 Winnebago Street, St. Louis, Missouri 63118. Former Federal employees' electronic Official Personnel Folders (eOPF) are located in the EHRI data system that is administered by NARA.

Note 1—The records in this system are records of the OPM and must be provided to those OPM employees who have an official need or use for those records. Therefore, if an employing agency is asked by an OPM employee to access the records within this system, such a request must be honored.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Current and former Federal employees as defined in 5 U.S.C. 2105.

(Volunteers, grantees, and contract employees on whom the agency maintains records may also be covered by this system).

CATEGORIES OF RECORDS IN THE SYSTEM:

All categories of records may include identifying information, such as name(s), date of birth, home address, mailing address, social security number, and home telephone. This system includes, but is not limited to, contents of the OPF as specified in OPM's Operating Manual, ''The Guide to Personnel Recordkeeping'' and OPM's ''Guide to Data Standards.'' Records in this system include:

a. Records reflecting work experience, education level achieved, and specialized education or training obtained outside of Federal service.

b. Records reflecting Federal service and documenting work experience and specialized education received while employed. Such records contain information about past and present positions held; grades; salaries; duty station locations; and notices of all personnel actions, such as appointments, transfers, reassignments, details, promotions, demotions, reductions-in-force, resignations, separations, suspensions, OPM approval of disability retirement applications, retirement, and removals.

c. Records on participation in the Federal Employees' Group Life Insurance Program and Federal Employees Health Benefits Program.

d. Records relating to an Intergovernmental Personnel Act assignment or Federal-private sector exchange program.

Note 2—Some of these records may also become part of the OPM/CENTRAL–5, Intergovernmental Personnel Act Assignment Record system.

e. Records relating to participation in an agency Federal Executive or Senior Executive Service (SES) Candidate Development Program.

Note 3—Some of these records may also become part of the OPM/Central-10 Federal Executive Institute Program Participant Records and OPM/CENTRAL–13 Executive Personnel Records systems.

f. Records relating to Government-sponsored training or participation in an agency's Upward Mobility Program or other personnel program designed to broaden an employee's work experiences and for purposes of advancement (e.g., an administrative intern program).

g. Records contained in the Enterprise Human Resource Integration (EHRI) and Central Personnel Data File (CPDF) maintained by OPM and exact substantive representations in agency manual or automated personnel information systems. These data elements include many of the above records along with disability, race/ethnicity, national origin, pay, and performance information from other OPM and agency systems of records. A definitive list of EHRI and CPDF data elements is contained in OPM's Operating Manuals, The Guide to Central Personnel Data File Reporting Requirements and The Guide to Personnel Data Standards.

h. Records on the SES maintained by agencies for use in making decisions affecting incumbents of these positions, e.g., relating to sabbatical leave programs, reassignments, and details, that are perhaps unique to the SES and that may be filed in the employee's OPF. These records may also serve as the basis for reports submitted to OPM for implementing OPM's oversight responsibilities concerning the SES.

i. Records on an employee's activities on behalf of the recognized labor organization representing agency employees, including accounting of official time spent and documentation in support of per diem and travel expenses.

Note 4—Alternatively, such records may be retained by an agency payroll office and thus be subject to the agency's internal Privacy Act system for payroll records. The OPM/GOVT–1 system does not cover general agency payroll records.

j. To the extent that the records listed here are also maintained in an agency electronic personnel or microform records system, those versions of these records are considered to be covered by this system notice. Any additional copies of these records (excluding performance ratings of record and conduct-related documents maintained by first line supervisors and managers covered by the OPM/GOVT–2 system) maintained by agencies at remote field/administrative offices from where the original records exist are considered part of this system.

Note 5—It is not the intent of OPM to limit this system of records only to those records physically within the OPF. Records may be filed in other folders located in offices other than where the OPF is located. Further, as indicated in the records location section, some of these records may be duplicated for maintenance at a site closer to where the employee works (e.g., in an administrative office or supervisors work folder) and still be covered by this system. In addition, a working file that a supervisor or other agency official is using that is derived from OPM/GOVT–1 is covered by this system notice. This system also includes working files derived from this notice that management is using in its personnel management capacity.

k. Records relating to designations for lump sum death benefits.

l. Records relating to classified information nondisclosure agreements.

m. Records relating to the Thrift Savings Plan (TSP) concerning the starting, changing, or stopping of contributions to the TSP as well as how the individual wants the investments to be made in the various TSP Funds.

Note 6—CPDF and EHRI data system's Central Employee Record (CER) are part of OPM/GOVT–1 system of records. CPDF and CER are highly reliable sources of statistical data on the workforce of the Federal government. However, the accuracy and completeness of each data element within the individual records that comprise the aggregate files are not guaranteed, and should not be used as the sole tool or as a substitute for the OPF in making personnel determinations or decisions concerning individuals.

Note 7—The eOPF Application within EHRI may contain documents and information beyond the scope and requirements of the OPF as documented in OPM's Guide to Personnel Recordkeeping. Those documents and information in the eOPF Application that are beyond the scope of the documented requirements are not considered part of the OPF or OPM/GOVT–1,

n. Records maintained in accordance with E.O. 13490, section 4(e), January 21, 2009. These records include the ethics pledges and all pledge waiver certifications with respect thereto.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM INCLUDES THE FOLLOWING WITH ANY REVISIONS OR AMENDMENTS:

5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.

Purposes:

The OPF, which may exist in various approved media, and other general personnel records files, is the official repository of the records, reports of personnel actions, and the documentation required in connection with these actions affected during an employee's Federal service. The personnel action reports and other documents, some of which are filed in the OPF, give legal force and effect to personnel transactions and establish employee rights and benefits under pertinent laws and regulations governing Federal employment.

These files and records are maintained by OPM and agencies in accordance with OPM regulations and instructions. They provide the basic source of factual data about a person's Federal employment while in the service and after his or her separation. Records in this system have various uses by agency personnel offices, including screening qualifications of employees; determining status, eligibility, and employee's rights and benefits under pertinent laws and regulations governing Federal employment; computing length of service; and other information needed to provide personnel services. These records may also be used to locate individuals for personnel research.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEMS, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

These records and information in these records may be used—

a. To disclose information to Government training facilities (Federal, State, and local) and to non-Government training facilities (private vendors of training courses or programs, private schools, etc.) for training purposes.

b. To disclose information to education institutions on appointment of a recent graduate to a position in the Federal service, and to provide college and university officials with information about their students working in the Student Career Experience Program, Volunteer Service, or other similar programs necessary to a student's obtaining credit for the experience gained.

c. To disclose information to officials of foreign governments for clearance before a Federal employee is assigned to that country.

d. To disclose information to the Department of Labor, Department of Veterans Affairs, Social Security Administration, Department of Defense, or any other Federal agencies that have special civilian employee retirement programs; or to a national, State, county, municipal, or other publicly recognized charitable or income security administration agency (e.g., State unemployment compensation agencies), when necessary to adjudicate a claim under the retirement, insurance, unemployment, or health benefits programs of the OPM or an agency cited above, or to an agency to conduct an analytical study or audit of benefits being paid under such programs.

e. To disclose information necessary to the Office of Federal Employees Group Life Insurance to verify election, declination, waiver of regular and/or optional life insurance coverage, or eligibility for payment of a claim for life insurance, or to TSP to verify election change and designation of beneficiary.

f. To disclose, to health insurance carriers contracting with OPM to provide a health benefits plan under the Federal Employees Health Benefits Program, information necessary to identify enrollment in a plan, to verify eligibility for payment of a claim for health benefits, or to carry out the coordination or audit of benefit provisions of such contracts.

g. To disclose information to a Federal, State, or local agency for determination of an individual's entitlement to benefits in connection with Federal Housing Administration programs.

h. To consider and select employees for incentive awards and other honors and to publicize those granted. This may include disclosure to other public and private organizations, including news media, which grant or publicize employee recognition.

i. To consider employees for recognition through quality-step increases and to publicize those granted. This may include disclosure to other public and private organizations, including news media, which grant or publicize employee recognition.

j. To disclose information to officials of labor organizations recognized under 5 U.S.C. chapter 71 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions.

Note 8—Home addresses will be released from this system only when there are no adequate, alternative sources available for this information.

k. To disclose pertinent information to the appropriate Federal, State, or local agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, when the disclosing agency becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation.

l. To disclose information to any source from which additional information is requested (to the extent necessary to identify the individual, inform the source of the purpose(s) of the request, and to identify the type of information requested), when necessary to obtain information relevant to an agency decision to hire or retain an employee, issue a security clearance, conduct a security or suitability investigation of an individual, classify jobs, let a contract, or issue a license, grant, or other benefits.

Note 9—When copies of records become part of an investigative process, those copies become subject to that systems' notice covering the investigative process i.e., if during an investigation, the OPM Federal Investigative Services Division makes copies of records contained in an Official Personnel Folder; those documents become part of OPM Central—9 Personnel Investigation Records system of records and are subject to that systems' routine uses.

m. To disclose to a Federal agency in the executive, legislative, or judicial branch of Government, in response to its request, or at the initiation of the agency maintaining the records, information in connection with the hiring of an employee, the issuance of a security clearance or determination concerning eligibility to hold a sensitive position, the conducting of an investigation for purposes of a credentialing, national security, fitness, or suitability adjudication concerning an individual, the classifying or designation of jobs, the letting of a contract, the issuance of a license, grant, or other benefit by the requesting agency, or the lawful statutory, administrative, or investigative purpose of the agency to the extent that the information is relevant and necessary to the requesting agency's decision.

n. To disclose information to the Office of Management and Budget at any stage in the legislative coordination and clearance process in connection with private relief legislation as set forth in OMB Circular No. A–19.

o. To provide information to a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual.

p. To disclose information to another Federal agency, to a court, or a party in litigation before a court or in an administrative proceeding being conducted by a Federal agency, when the Government is a party to the judicial or administrative proceeding.

q. To disclose information to the Department of Justice, or in a proceeding before a court, adjudicative body, or other administrative body before which the agency is authorized to appear, when:

1. The agency, or any component thereof; or

2. Any employee of the agency in his or her official capacity; or

3. Any employee of the agency in his or her individual capacity where the Department of Justice or the agency has agreed to represent the employee; or

4. The United States, when the agency determines that litigation is likely to affect the agency or any of its components, is a party to litigation or has an interest in such litigation, and the use of such records by the Department of Justice or the agency is deemed by the agency to be relevant and necessary to the litigation provided, however, that in each case it has been determined that the disclosure is compatible with the purpose for which the records were collected.

r. By the National Archives and Records Administration in records management inspections and its role as Archivist.

s. By the agency maintaining the records or by the OPM to locate individuals for personnel research or survey response, and in the production of summary descriptive statistics and analytical studies in support of the function for which the records are collected and maintained, or for related workforce studies. While published statistics and studies do not contain individual identifiers, in some instances, the selection of elements of data included in the study may be structured in such a way as to make the data individually identifiable by inference.

t. To provide an official of another Federal agency information needed in the performance of official duties related to reconciling or reconstructing data files, in support of the functions for which the records were collected and maintained.

u. When an individual to whom a record pertains is mentally incompetent or under other legal disability, to provide information in the individual's record to any person who is responsible for the care of the individual, to the extent necessary to assure payment of benefits to which the individual is entitled.

v. To disclose to the agency-appointed representative of an employee all notices, determinations, decisions, or other written communications issued to the employee in connection with an examination ordered by the agency under fitness-for-duty examination procedures.

w. To disclose, in response to a request for discovery or for appearance of a witness, information that is relevant to the subject matter involved in a pending judicial or administrative proceeding.

x. To disclose to a requesting agency, organization, or individual the home address and other relevant information on those individuals who it reasonably believed might have contracted an illness or might have been exposed to or suffered from a health hazard while employed in the Federal workforce.

y. To disclose specific civil service employment information required under law by the Department of Defense on individuals identified as members of the Ready Reserve to assure continuous mobilization readiness of Ready Reserve units and members, and to identify demographic characteristics of civil service retirees for national emergency mobilization purposes.

z. To disclose information to the Department of Defense, National Oceanic and Atmospheric Administration, U.S. Public Health Service, Department of Veterans Affairs, and the U.S. Coast Guard needed to effect any adjustments in retired or retained pay required by the dual compensation provisions of section 5532 of title 5, United States Code.

aa. To disclose information to the Merit Systems Protection Board or the Office of the Special Counsel in connection with appeals, special studies of the civil service and other merit systems, review of OPM rules and regulations, investigation of alleged or possible prohibited personnel practices, and such other functions promulgated in 5 U.S.C. chapter 12, or as may be authorized by law.

bb. To disclose information to the Equal Employment Opportunity Commission when requested in connection with investigations of alleged or possible discrimination practices in the Federal sector, examination of Federal affirmative employment programs, compliance by Federal agencies with the Uniform Guidelines on Employee Selection Procedures, or other functions vested in the Commission.

cc. To disclose information to the Federal Labor Relations Authority (including its General Counsel) when requested in connection with investigation and resolution of allegations of unfair labor practices, in connection with the resolution of exceptions to arbitrator's awards when a question of material fact is raised, to investigate representation petitions and to conduct or supervise representation elections, and in connection with matters before the Federal Service Impasses Panel.

dd. To disclose to prospective non-Federal employers, the following information about a specifically identified current or former Federal employee:

(1) Tenure of employment;

(2) Civil service status;

(3) Length of service in the agency and the Government; and

(4) When separated, the date and nature of action as shown on the Notification of Personnel Action—Standard Form 50 (or authorized exception).

ee. To disclose information on employees of Federal health care facilities to private sector (i.e., other than Federal, State, or local government) agencies, boards, or commissions (e.g., the Joint Commission on Accreditation of Hospitals). Such disclosures will be made only when the disclosing agency determines that it is in the Government's best interest (e.g., to comply with law, rule, or regulation, to assist in the recruiting of staff in the community where the facility operates to obtain accreditation or other approval rating, or to avoid any adverse publicity that may result from public criticism of the facility's failure to obtain such approval). Disclosure is to be made only to the extent that the information disclosed is relevant and necessary for that purpose.

ff. To disclose information to any member of an agency's Performance Review Board, Executive Resources Board, or other panel when the member is not an official of the employing agency; information would then be used for approving or recommending selection of candidates for executive development or SES candidate programs, issuing a performance rating of record, issuing performance awards, nominating for meritorious or distinguished executive ranks, or removal, reduction-in-grade, or other personnel actions based on performance.

gg. To disclose, either to the Federal Acquisition Institute (FAI) or its agent, information about Federal employees in procurement occupations and other occupations whose incumbents spend the predominant amount of their work hours on procurement tasks; provided that the information shall be used only for such purposes and under such conditions as prescribed by the notice of the Federal Acquisition Personnel Information System as published in the **Federal Register** of February 7, 1980 (45 FR 8399).

hh. To disclose relevant information with personal identifiers of Federal civilian employees whose records are contained in the EHRI to authorized Federal agencies and non-Federal entities for use in computer matching. The matches will be performed to help eliminate waste, fraud, and abuse in Governmental programs; to help identify individuals who are potentially in violation of civil or criminal law or regulation; and to collect debts and overpayments owed to Federal, State, or local governments and their components. The information disclosed may include, but is not limited to, the name, social security number, date of birth, sex, annualized salary rate, service computation date of basic active service, veteran's preference, retirement status, occupational series, health plan code, position occupied, work schedule (full time, part time, or intermittent), agency identifier, geographic location (duty station location), standard metropolitan service area, special program identifier, and submitting office number of Federal employees.

ii. To disclose information to Federal, State, local, and professional licensing boards, Boards of Medical Examiners, or to the Federation of State Medical Boards or a similar non-government entity which maintains records concerning individuals' employment histories or concerning the issuance, retention or revocation of licenses, certifications or registration necessary to practice an occupation, profession or specialty, to obtain information relevant to an Agency decision concerning the hiring, retention, or termination of an employee or to inform a Federal agency or licensing boards or the appropriate non-government entities about the health care practices of a terminated, resigned or retired health care employee whose professional health care activity so significantly failed to conform to generally accepted standards of professional medical practice as to raise reasonable concern for the health and safety of patients in the private sector or from another Federal agency.

jj. To disclose information to contractors, grantees, or volunteers performing or working on a contract, service, grant, cooperative agreement, or job for the Federal Government.

kk. To disclose information to a Federal, State, or local governmental entity or agency (or its agent) when necessary to locate individuals who are owed money or property either by a Federal, State, or local agency, or by a financial or similar institution.

ll. To disclose to a spouse or dependent child (or court-appointed guardian thereof) of a Federal employee enrolled in the Federal Employees Health Benefits Program, upon request, whether the employee has changed from a self-and-family to a self-only health benefits enrollment.

mm. To disclose information to the Office of Child Support Enforcement, Administration for Children and Families, Department of Health and Human Services, Federal Parent Locator System, or Federal Offset System for use in locating individuals, verifying social security numbers, or identifying their incomes sources to establish paternity, establish, or modify orders of support and for enforcement action.

nn. To disclose records on former Panama Canal Commission employees to the Republic of Panama for use in employment matters.

oo. To disclose to appropriate Federal officials pertinent workforce information for use in national or homeland security emergency/disaster response.

pp. To disclose on public and internally-accessible Federal Government Web sites, and to otherwise disclose to any person, including other departments and agencies, the signed ethics pledges and pledge waiver certifications issued under E.O. 13490 of January 21, 2009, Ethics Commitments by Executive Branch Personnel.

qq. To disclose foreign language proficiencies to Federal agencies in support of the National Preparedness Goal and the Presidential Policy Directive 8 (PPD–8).

rr. To disclose information to the Centers for Medicare and Medicaid (CMS) to assist in determining whether individuals are eligible for programs under the Patient Protection and Affordable Care Act (PPACA).

POLICIES AND PRACTICES OF STORING, RETRIEVING, SAFEGUARDING, AND RETAINING AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

These records are maintained in file folders, on lists and forms, microfilm or microfiche, and in computer processable storage media such as personnel system databases, PDF forms and data warehouse systems.

RETRIEVABILITY:

These records are retrieved by various combinations of name, agency, birth date, social security number, or identification number of the individual on whom they are maintained.

SAFEGUARDS:

Paper or microfiche/microfilmed records are located in locked metal file cabinets or in secured rooms with access limited to those personnel whose official duties require access. Access to computerized records is limited, through use of user logins and passwords, access codes, and entry logs, to those whose official duties require access. Computerized records systems are consistent with the requirements of the Federal Information Security Management Act (Pub. L. 107–296), and associated OMB policies, standards and guidance from the National Institute of Standards and Technology.

RETENTION AND DISPOSAL:

The OPF is maintained for the period of the employee's service in the agency and is then, if in a paper format, transferred to the National Personnel Records Center for storage or, as appropriate, to the next employing Federal agency. If the OPF is maintained in an electronic format, the transfer and storage is in accordance with the OPM approved electronic system. Other records are either retained at the agency for various lengths of time in accordance with the National Archives and Records Administration records schedules or destroyed when they have served their purpose or when the employee leaves the agency. The transfer occurs within 90 days of the individuals' separation. In the case of administrative need, a retired employee, or an employee who dies in service, the OPF is sent within 120 days. Destruction of the OPF is in accordance with General Records Schedule-1 (GRS–1) or GRS 20.

Records contained within the CPDF and EHRI (and in agency's automated personnel records) may be retained indefinitely as a basis for longitudinal work history statistical studies. After the disposition date in GRS–1 or GRS 20, such records should not be used in making decisions concerning employees.

SYSTEM MANAGER AND ADDRESS:

a. Manager, OCIO/RM, U.S. Office of Personnel Management, 1900 E Street NW., Washington, DC 20415.

b. For current Federal employees, OPM has delegated to the employing agency the Privacy Act responsibilities concerning access, amendment, and disclosure of the records within this system notice.

NOTIFICATION PROCEDURE:

Individuals wishing to inquire whether this system of records contains information about them should contact the appropriate OPM or employing agency office, as follows:

a. Current Federal employees should contact the Personnel Officer or other responsible official (as designated by the employing agency), of the local agency installation at which employed regarding records in this system.

b. Former Federal employees who want access to their Official Personnel Folders (OPF) should contact the National Personnel Records Center (Civilian), 111 Winnebago Street, St. Louis, Missouri 63118, regarding the records in this system. For other records covered by the system notice, individuals should contact their former employing agency. Individuals must furnish the following information for their records to be located and identified:

a. Full name.
b. Date of birth.
c. Social security number.
d. Last employing agency (including duty station) and approximate date(s) of the employment (for former Federal employees).
e. Signature.

RECORD ACCESS PROCEDURE:

Individuals wishing to request access to their records should contact the appropriate OPM or agency office, as specified in the Notification Procedure section. Individuals must furnish the following information for their records to be located and identified:

a. Full name(s).
b. Date of birth.
c. Social security number.
d. Last employing agency (including duty station) and approximate date(s) of employment (for former Federal employees).
e. Signature.

Individuals requesting access must also comply with the Office's Privacy Act regulations on verification of identity and access to records (5 CFR part 297).

CONTESTING RECORD PROCEDURE:

Current employees wishing to request amendment of their records should contact their current agency. Former employees should contact the system manager. Individuals must furnish the following information for their records to be located and identified.

a. Full name(s).
b. Date of birth.
c. Social security number.
d. Last employing agency (including duty station) and approximate date(s) of employment (for former Federal employees).
e. Signature.

Individuals requesting amendment must also comply with the Office's Privacy Act regulations on verification of identity and amendment of records (5 CFR part 297).

RECORD SOURCE CATEGORIES:

Information in this system of records is provided by—

a. The individual on whom the record is maintained.
b. Educational institutions.
c. Agency officials and other individuals or entities.
d. Other sources of information maintained in an employee's OPF, in accordance with Code of Federal Regulations Part 293, and OPM's Operating Manual, ''The Guide to Personnel Recordkeeping.''

[FR Doc. 2012–29777 Filed 12–10–12; 8:45 am]

BILLING CODE 6325–45–P

POSTAL REGULATORY COMMISSION

[Docket No. CP2013–24; Order No. 1566]

International Mail Contract

AGENCY: Postal Regulatory Commission.

ACTION: Notice.

SUMMARY: The Commission is noticing a recent Postal Service filing concerning an additional inbound competitive Multi-Service Agreements with Foreign Postal Operators 1 negotiated service agreement with Royal PostNL BV. This notice informs the public of the filing, invites public comment, and takes other administrative steps.

DATES: *Comments are due:* December 14, 2012.

ADDRESSES: Submit comments electronically via the Commission's Filing Online system at *http://www.prc.gov.* Those who cannot submit comments electronically should contact the person identified in the **FOR FURTHER INFORMATION CONTACT** section by telephone for advice on filing alternatives.

FOR FURTHER INFORMATION CONTACT: Stephen L. Sharfman, General Counsel, at 202–789–6820.

SUPPLEMENTARY INFORMATION:

Table of Contents

I. Introduction
II. Contents of Filing
III. Commission Action
IV. Ordering Paragraphs

I. Introduction

On December 4, 2012, the Postal Service filed a notice, pursuant to 39 CFR 3015.5, stating that it has entered into an additional negotiated service agreement (Agreement) with the Netherlands' foreign postal operator Royal PostNL BV (PostNL).[1] The Postal Service seeks to have the inbound portion of the Agreement, which concerns delivery of inbound Air CP [2] and EMS in the United States, included within the Inbound Competitive Multi-Service Agreements with Foreign Postal Operators 1 (MC2010–34) product on the competitive product list. Notice at 1.

II. Contents of Filing

The Postal Service's filing consists of the Notice, a public Excel file containing redacted financial workpapers, and four attachments. Attachment 1 is a redacted copy of the Agreement. *Id.* at 3. Attachment 2 is the certified statement required by 39 CFR 3015.5(c)(2). *Id.* Attachment 3 is a redacted copy of the Governors' Decision No. 10–3. *Id.* Attachment 4 is an application for non-public treatment of unredacted material. *Id.* The Agreement's intended effective date is January 1, 2013. *Id.* at 4.

The rates for inbound Air CP and EMS included in the Agreement are to remain in effect for 2 years after the Agreement's effective date, unless terminated sooner. *Id.* The Postal Service further notes that a TNT Agreement, in accordance with Article 22 of the TNT Agreement, automatically renewed on October 1, 2012, but pursuant to paragraph 3 of Article 22 of the PostNL Agreement, the TNT Agreement is to expire the day prior to the effective date of the PostNL Agreement, if an effective date for the PostNL agreement is established. *Id.* at 3 n.5.

The Postal Service reviews the regulatory history of the Inbound Competitive Multi-Service Agreements with Foreign Operators 1 product and identifies the TNT Agreement (approved in Docket No. CP2010–95) as the baseline agreement for purposes of determining the functional equivalence of the instant Agreement.[3] *Id.* at 2. It asserts that the instant Agreement fits within applicable Mail Classification Schedule language and addresses functional equivalency with the baseline agreement, including similarity of cost characteristics. *Id.* at 3–7. The Postal Service also identifies differences between the two contracts, such as the addition of several articles, revisions to existing articles, and new annexes, but asserts that these differences do not detract from a finding of functional equivalency. *Id.* at 5–7.

III. Commission Action

Notice of establishment of docket. The Commission establishes Docket No. CP2013–24 for consideration of matters

[1] Notice of United States Postal Service of Filing Functionally Equivalent Inbound Competitive Multi-Service Agreement with a Foreign Postal Operator, December 4, 2012 (Notice).

[2] ''CP'' is an abbreviation used to identify or reference international parcel post (from the French phrase *colis postaux,* ''postal package'').

[3] The Postal Service identifies Governors' Decision No. 10–3 as the enabling Governors' Decision. *Id.* at 5. The status of the TNT Agreement as the baseline agreement was confirmed in Docket No. CP2011–69, Order No. 840, Order Concerning an Additional Inbound Competitive Multi-Service Agreements with Foreign Postal Operators 1 Negotiated Service Agreement, September 7, 2011. *See id.* at 2.

OPM/GOVT–2

System Name:

Employee Performance File System Records.

System Location:

Records maintained in this system may be located as follows:

a. In an Employee Performance File (EPF) maintained in the agency office responsible for maintenance of the employee's Official Personnel Folder (OPF) or other agency-designated office. This includes those instances where the agency uses an envelope within the OPF in lieu of a separate EPF folder.

b. In the EPF of Senior Executive Service (SES) appointees where the agency elects to have the file maintained by the Performance Review Boards required by 5 U.S.C. 4314(c)(1), or the administrative office supporting the Board.

c. In any supervisor/manager's work folder maintained in the office by the employee's immediate supervisor/manager or, where agencies have determined that records management is better served, in such folders maintained for supervisors/managers in a central administrative office.

d. In an agency's electronic personnel records system.

e. In an agency microformed EPF.

Note 1:

Originals or copies of records covered by this system may be located in more than one location, but if they become part of an agency internal system (e.g., administrative or negotiated grievance file), those copies then would be subject to the agency's internal Privacy Act implementation guidance regarding their use within the agency's system.

Note 2:

The records in this system are ‘owned’ by the Office of Personnel Management (OPM) and should be provided to those Office employees who have an official need or use for those records. Therefore, if an employing agency is asked by an OPM employee for access to the records within this system, such a request should be honored.

Categories of Individuals Covered by the System:

Current and former Federal employees (including SES appointees).

Categories of Records in the System:

Records in this system, wherever they are maintained, may include any or all of the following:

a. Annual summary performance ratings of record issued under employee appraisal systems and any document that indicates that the rating is being challenged under administrative procedures (e.g., when the employee files a grievance on the rating received).

b. A document (either the summary rating form itself or a form affixed to it) that identifies the job elements and the standards for those elements upon which the rating is based.

c. Supporting documentation for employee ratings of records, as required by agency rating systems or implementing instructions, and which may be filed physically with the rating of record (e.g., productivity and quality control records, records of employee counseling, individual development plans, or other such records as specified in agency issuances) and maintained, for example in a work folder by supervisors/managers at the work site.

d. Records on SES appraisals generated by Performance Review Boards, including statements of witnesses and transcripts of hearings.

e. Written recommendations for awards, removals, demotions, denials of within-grade increases, reassignments, training, pay increases, cash bonuses, or other performance-based actions (e.g., nominations of SES employees for Meritorious or Distinguished Executive), including supporting documentation.

f. Statements made (letter on or appended to the performance rating document) by the employee (e.g., a statement of disagreement with the rating or recommendation), in accordance with agency performance plans and implementing instructions, regarding a rating given and any recommendations made based on them.

Note 3:

When a recommendation by a supervisor/manager or a statement made by the employee regarding the rating issued (or a copy) becomes part of another Governmentwide system or internal agency file (e.g., an SF 52 when the action is effected or when documents or statements of disagreement are placed in a grievance file), that document then becomes subject to that system's notice and appropriate OPM or employing agency Privacy Act requirements, respectively, for the system of records covering that file.

g. Records created by Executive Resource Boards regarding performance of an individual in an executive development program.

h. Records concerning performance during the supervisory or managerial probationary period, the SES appointment probationary period, or the employee's initial period of probation after appointment.

i. Notices of commendations, recommendations for training, such as an Individual Development Plan, and advice and counseling records that are based on work performance.

j. Copies of supervisory ratings used in considering employees for promotion or other position changes originated in conjunction with agency merit promotion programs when specifically authorized for retention in the EPF or work folder.

k. Performance-related material that may be maintained in the work folder to assist the supervisor/manager in accurately assessing employee performance. Such material may include transcripts of employment and training history, documentation of special licenses, certificates, or authorizations necessary in the performance of the employee duties, and other such records that agencies determine to be appropriate for retention in the work folder.

l. Standard Form 7B cards. (While the use of the SF 7B Card system was cancelled effective December 31, 1992, this system notice will cover any of those cards still in existence.)

Note 4:

To the extent that performance records covered by this system are maintained in either an EPF, supervisor/manager work folder, or an agency's electronic or microform record system, they are considered covered under this system of records. Further, when copies of records filed in the employee's OPF are maintained as general records related to performance (item k above), those records are to be considered as being covered by this system and not the OPM/GOVT–1 system.

This notice does not cover these records (or copies) when they become part of a grievance file or a 5 CFR parts 432, 752, or 754 file (documents maintained in these files are covered by the OPM/GOVT–3 system of records, while grievance records are covered under an agency-specific system), or when they become part of an appeal or discrimination complaint file as such documents are considered to be part of either the system of appeal records under the control of the Merit Systems Protection Board (MSPB) or discrimination complaints files under the control of the Equal Employment Opportunity Commission (EEOC).

When an agency retains copies of records from this system in another system of records, not covered by this or another OPM, MSPB, or EEOC Government-wide system notice, the agency is solely responsible for responding to any Privacy Act issues raised concerning these documents.

The Office has adopted a position that when supervisors/managers retain personal "supervisory" notes, i.e., information on employees that the agency exercises no control and does not require or specifically describe in its performance system, which remain solely for the personal use of the author and are not provided to any other person, and which are retained or discarded at the author's sole discretion, such notes are not subject to the Privacy Act and are, therefore, not considered part of this system. Should an agency choose to adopt a position that such notes are subject to the Act, that agency is solely responsible for dealing with Privacy Act matters, including the requisite system notice, concerning them.

Authority for Maintenance of the System:

Sections 1104, 3321, 4305, and 5405 of title 5, U.S. Code, and Executive Order 12107.

Purpose:

These records are maintained to ensure that all appropriate records on an employee's performance are retained and are available (1) To agency officials having a need for the information; (2) to employees; (3) to support actions based on the records; (4) for use by the OPM in connection with its personnel management evaluation role in the executive branch; and (5) to identify individuals for personnel research.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purpose of Such Uses:

a. To disclose information to the Merit Systems Protection Board or the Office of Special Counsel in connection with appeals, special studies of the civil service and other merit systems, review of Office rules and regulations, investigations of alleged or possible prohibited personnel practices, and other functions as promulgated in 5 U.S.C. chapter 12, or for such other functions as may be authorized by law.

b. To disclose information to the EEOC when requested in connection with investigations into alleged or possible discrimination practices in the Federal sector, examination of Federal Affirmative Action programs, compliance by Federal agencies with the Uniform Guidelines on Employee Selection Procedures, or other functions vested in the Commission.

c. To disclose information to the Federal Labor Relations Authority (including its General Counsel) when requested in connection with the investigation and resolution of allegations of unfair labor practices, in connection with the resolution of exceptions to arbitrator's awards where a question of material fact is raised, and matters before the Federal Service Impasses Panel.

d. To consider and select employees for incentive awards, quality-step increases, merit increases and performance awards, or other pay bonuses, and other honors and to publicize those granted. This may include disclosure to public and private organizations, including news media, which grant or publicize employee awards or honors.

e. To disclose information to an arbitrator to resolve disputes under a negotiated grievance procedure or to officials of labor organizations recognized under 5 U.S.C. chapter 71 when relevant and necessary to their duties of exclusive representation.

f. To disclose to an agency in the executive, legislative, or judicial branch, or to the District of Columbia's government in response to its request, or at the initiation of the agency maintaining the records, information in connection with hiring or retaining of an employee; issuing a security clearance; conducting a security or suitability investigation of an individual; classifying jobs; letting a contract; issuing a license, grant, or other benefits by the requesting agency; or the lawful statutory, administrative, or investigative purposes of the agency to the extent that the information is relevant and necessary to the decision on the matter.

g. To disclose, in response to a request for discovery or for appearance of a witness, information that is relevant to the subject matter involved in a pending judicial or administrative proceeding.

h. To disclose information to a congressional office from the record or an individual in response to an inquiry from that congressional office made at the request of the individual.

i. To disclose information to another Federal agency, to a court, or a party in litigation before a court or in an administrative proceeding being conducted by a Federal agency, when the Government is a party to the judicial or administrative proceeding.

j. To disclose information to the Department of Justice, or in a proceeding before a court, adjudicative body, or other administrative body before which the agency is authorized to appear, when:

1. The agency, or any component thereof; or

2. Any employee of the agency in his or her official capacity; or

3. Any employee of the agency in his or her individual capacity where the Department of Justice or the agency has agreed to represent the employee; or

4. The United States, when the agency determines that litigation is likely to affect the agency or any of its components, is a party to litigation or has an interest in such litigation, and the use of such records by the Department of Justice or the agency is deemed by the agency to be relevant and necessary to the litigation, provided, however, that in each case it has been determined that the disclosure is compatible with the purpose for which the records were collected.

k. By the National Archives and Records Administration in records management inspections and its role as Archivist.

l. By the OPM or employing agency to locate individuals for personnel research or survey response and in producing summary descriptive statistics and analytical studies to support the function for which the records are collected and maintained, or for related workforce studies. While published statistics and studies do not contain individual identifiers, in some instances the selection of elements of data included in the study may be structured in such a way as to make the data individually identifiable by inference.

m. To disclose pertinent information to the appropriate Federal, State, or local government agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, where the agency maintaining the record becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation.

n. To disclose information to any member of an agency's Performance Review Board or other board or panel when the member is not an official of the employing agency. The information would then be used for approving or recommending performance awards, nominating for meritorious and distinguished executive ranks, and removal, reduction-in-grade, and other personnel actions based on performance.

o. To disclose to Federal, State, local, and professional licensing boards or Boards of Medical Examiners, when such records reflect on the qualifications of individuals seeking to be licensed.

p. To disclose to contractors, grantees, or volunteers performing or working on a contract, service, grant, cooperative agreement, or job for the Federal Government.

q. To disclose records on former Panama Canal Commission employees to the Republic of Panama for use in employment matters.

Policies and Practices for Storing, Retrieving, Safeguarding, Retaining and Disposing of Records in the System:

Storage:

Records are maintained in file folders, envelopes, and on magnetic tapes, disks, microfilm, or microfiche.

Retrievability:

Records are retrieved by the name and social security number of the individual on whom they are maintained.

Safeguards:

Records are maintained in file folders or envelopes, on electronic media, magnetic tape, disks, or microforms and are stored in locked desks, metal filing cabinets, or in a secured room with access limited to those whose official duties require access. Additional safeguarding procedures include the use of sign-out sheets and restrictions on the number of employees able to access electronic records through use of access codes and logs.

Retention and Disposal:

Records on former non-SES employees will generally be retained no longer than 1 year after the employee leaves his or her employing agency. Records on former SES employees may be retained up to 5 years under 5 U.S.C. 4314.

a. Summary performance appraisals (and related records as the agency prescribes) on SES appointees are retained for 5 years and ratings of record on other employees for 4 years, except as shown in paragraph b. below, and are disposed of by shredding, burning, erasing of disks, or in accordance with agency procedures regarding destruction of personnel records, including giving them to the individual. When a non-SES employee transfers to another agency or leaves Federal employment, ratings of record and subsequent ratings (4 years old or less) are to be filed on the temporary side of the OPF and forwarded with the OPF.

b. Ratings of unacceptable performance and related documents, pursuant to 5 U.S.C. 4303(d), are destroyed after the employee completes 1 year of acceptable performance from the date of the proposed removal or reduction-in-grade notice. (Destruction to be no later than 30 days after the year is up.)

c. When a career appointee in the SES accepts a Presidential appointment pursuant to 5 U.S.C. 3392(c), the employee's performance folder remains active so long as the employee remains employed under the Presidential appointment and elects to have certain provisions of 5 U.S.C. relating to the Service apply.

d. When an incumbent of the SES transfers to another position in the Service, ratings and plans 5 years old or less shall be forwarded to the gaining agency with the individual's OPF.

e. Some performance-related records (e.g., documents maintained to assist rating officials in appraising performance or recommending remedial actions or to show that the employee is currently licensed or certified) may be destroyed after 1 year.

f. Where any of these documents are needed in connection with administrative or negotiated grievance procedures, or quasi-judicial or judicial proceedings, they may be retained as needed beyond the retention schedules identified above.

g. Generally, agencies retain records on former employees for no longer than 1 year after the employee leaves.

Note 5:

When an agency retains an electronic or microform version of any of the above documents, retention of such records longer than shown is permitted (except for those records subject to 5 U.S.C. 4303(d)) for agency use or for historical or statistical analysis, but only so long as the record is not used in a determination directly affecting the individual about whom the record pertains (after the manual record has been or should have been destroyed).

System Manager(s) and Address:

a. Deputy Associate Director, Center for HR Systems Requirements and Strategies, Room 6H31, U.S. Office of Personnel Management, 1900 E Street, NW., Washington, DC 20415.

b. For current Federal employees, OPM has delegated to the employing agency the Privacy Act responsibilities concerning access, amendment, and disclosure of the record within this system notice.

Notification Procedure:

Individuals wishing to inquire whether this system contains information about them should contact their servicing personnel office, supervisor/manager, Performance Review Board office, or other agency designated office maintaining their performance-related records where they are or were employed. Individuals must furnish the following information for their records to be located and identified:

a. Full name(s).

b. Social Security number.

c. Position occupied and unit where employed.

Records Access Procedure:

Individuals wishing access to their records should contact the appropriate office indicated in the Notification Procedure section where they are or were employed. Individuals must furnish the following information for their records to be located and identified:

a. Full name(s).

b. Social security number.

c. Position occupied and unit where employed.

Individuals requesting access to records must also comply with the OPM's Privacy Act regulations on verification of identity and access to records (5 CFR part 297).

Contesting Record Procedure:

Individuals wishing to request amendment to their records should contact the appropriate office indicated in the Notification Procedure section where they are or were employed. Individuals must furnish the following information for their records to be located and identified:

a. Full name(s).

b. Social security number.

c. Position occupied and unit where employed.

Individuals requesting amendment must also comply with the OPM's Privacy Act regulations on verification of identity and amendment of records (5 CFR part 297).

Records Source Categories:

Records in this system are obtained from:

a. Supervisors/managers.

b. Performance Review Boards.

c. Executive Resource Boards.

d. Other individuals or agency officials.

e. Other agency records.

f. The individual to whom the records pertain.

Ridge, Tennessee. Hermes would be a fluoride-salt cooled, high-temperature reactor that uses solid tri-structural isotropic fuel in pebble form. A notice of receipt and availability of this portion of the application was published in the **Federal Register** on October 29, 2021 (86 FR 60077).

The first part of the Kairos construction permit application consisted of the following information:

• The general information required by 10 CFR 50.33.

• The Preliminary Safety Analysis Report required by 10 CFR 50.34(a).

• Exemption requests to support issuance of a construction permit.

• A request to invoice the filing fee required by 10 CFR 50.30(e) and 10 CFR 170.21.

On October 31, 2021, Kairos filed the second part of its application (ADAMS Package Accession No. ML21306A131) for a construction permit, which consisted of the Environmental Report required by 10 CFR 50.30(f). Submission of the Environmental Report completed the application for a construction permit.

The NRC staff determined that Kairos submitted a two-part application in accordance with 10 CFR 2.101(a)(5) and 10 CFR part 50, and that the application is acceptable for docketing under Docket No. 50–7513. The NRC staff provided Kairos notice of the acceptance and docketing determinations by letter dated November 29, 2021 (ADAMS Accession No. ML21319A354).

The NRC staff will perform a detailed technical review of the construction permit application and document its safety findings in a safety evaluation report. Also, in accordance with 10 CFR part 51, ''Environmental Protection Regulations for Domestic Licensing and Related Regulatory Functions,'' the NRC staff will prepare an environmental impact statement for the proposed action.

Docketing of the application does not preclude the NRC from requesting additional information from the applicant as the review proceeds, nor does it predict whether the Commission will grant or deny the application. The construction permit application will be referred to the Advisory Committee on Reactor Safeguards for review and report consistent with 10 CFR 50.58, ''Hearings and report of the Advisory Committee on Reactor Safeguards.'' If, after holding an evidentiary hearing, the Commission finds that the construction permit application meets the applicable standards of the Atomic Energy Act and the Commission's regulations, and that any required notifications to other agencies and bodies have been made, the Commission will issue a construction permit, in the form and containing conditions and limitations that the Commission finds appropriate and necessary.

The Commission will announce, in a future **Federal Register** notice, the opportunity to petition for leave to intervene in a proceeding on the construction permit application.

Dated: November 24, 2021.

For the Nuclear Regulatory Commission.

Benjamin G. Beasley,

Senior Project Manager, Advanced Reactor Licensing Branch, Division of Advanced Reactors and Non-Power Production and Utilization Facilities, Office of Nuclear Reactor Regulation.

[FR Doc. 2021–26119 Filed 11–30–21; 8:45 am]

BILLING CODE 7590–01–P

OFFICE OF PERSONNEL MANAGEMENT

Privacy Act of 1974; System of Records

AGENCY: Office of Personnel Management.

ACTION: Notice of a modified system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Office of Personnel Management (''OPM''), proposes to modify an OPM government-wide system of records, OPM/GOVT–5, Recruiting, Examining, and Placement Records, primarily to make clear that records collected and generated in the process of onboarding Federal employees but prior to their entry-on-duty date are included in this system of records. In addition, OPM proposes additional administrative changes to reflect the current OPM organization.

DATES: Please submit comments on or before January 3, 2022. This modified system of records is effective upon publication.

ADDRESSES: You may submit written comments through the Federal Rulemaking Portal: *http://www.regulations.gov.* All submissions received must include the agency name and docket number for this **Federal Register** document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the internet at *http://www.regulations.gov* as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Dianna Saxman, Associate Director, Human Resources Solutions, Office of Personnel Management at *Dianna.Saxman@opm.gov.* For privacy questions, please contact: Kellie Cosgrove Riley, Chief Privacy Officer, Office of Personnel Management at 202–360–6065 or *privacy@opm.gov.*

SUPPLEMENTARY INFORMATION: In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Office of Personnel Management (''OPM''), proposes to make certain modifications to the OPM/GOVT–5 Recruiting, Examining, and Placement Records system of records pending a comprehensive review and update at a later date. The records in this system of records include all records submitted by an applicant for Federal employment or generated in connection with the application and the onboarding process.

OPM proposes to modify this system of records to add an additional category of records: ''m. Records collected or generated in the process of onboarding an applicant selected to fill a vacant position, to include, for example, vaccination records, proof of citizenship, and agency-specific documentation necessary for the onboarding process.'' This category of records is being added to clarify that records collected or generated in the onboarding process, after applicants have been selected but before they are Federal employees, are included in this system of records. Once an individual completes the onboarding process and is a Federal employee, certain records collected and generated in the onboarding process may be included in other systems of records. For example, proof of vaccination required by Executive Order 14043, Requiring Coronavirus Disease 2019 Vaccination for Federal Employees, may later be included in the OPM/GOVT–10 Employee Medical File Systems Records system of records; and personnel forms completed in the onboarding process may later be included in the OPM/GOVT–1 General Personnel Records system of records.

In addition to modifying this system of records to add an additional category of records, OPM also proposes to modify the description of the system location and identification of the system manager. Both modifications are being made to reflect organizational changes at OPM since the last publication of the OPM/GOVT–5 system of records notice.

OPM has provided a report of this modified system of records to the Committee on Oversight and

Government Reform of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Office of Management and Budget (OMB), pursuant to 5 U.S.C. 552a(r) and OMB Circular A–108, ''Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act,'' dated December 23, 2016. This modified system of records will be included in OPM's inventory of record systems.

Alexys Stanley,

Regulatory Affairs Analyst.

SYSTEM NAME AND NUMBER:

Recruiting, Examining, and Placement Records, OPM/GOVT–5.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Human Resources Solutions, Office of Personnel Management, 1900 E Street NW, Washington, DC 20415, has government-wide responsibility for the records in this system of records. Individual agencies have responsibility for the records pertaining to their applicants.

SYSTEM MANAGER(S):

Associate Director, Human Resources Solutions, U.S. Office of Personnel Management, 1900 E Street NW, Room 6H31, Washington, DC 20415.

CATEGORIES OF RECORDS IN THE SYSTEM:

* * * * *

m. Records collected or generated in the process of onboarding an applicant selected to fill a vacant position, to include, for example, vaccination records, proof of citizenship, and agency-specific documentation necessary for the onboarding process.

* * * * *

HISTORY:

61 FR 36919 (July 15, 1996); 65 FR 24731 (April 27, 2000); 71 FR 35341 (June 19, 2006); 79 FR 16834 (March 26, 2014); 80 FR 74815 (November 30, 2015).

[FR Doc. 2021–26086 Filed 11–30–21; 8:45 am]

BILLING CODE 6325–43–P

SECURITIES AND EXCHANGE COMMISSION

[Investment Company Act Release No. 34426]

Notice of Applications for Deregistration Under Section 8(f) of the Investment Company Act of 1940

November 26, 2021.

The following is a notice of applications for deregistration under section 8(f) of the Investment Company Act of 1940 for the month of November 2021. A copy of each application may be obtained via the Commission's website by searching for the file number, or for an applicant using the Company name box, at *http://www.sec.gov/search/search.htm* or by calling (202) 551–8090. An order granting each application will be issued unless the SEC orders a hearing. Interested persons may request a hearing on any application by emailing the SEC's Secretary at *Secretarys-Office@sec.gov* and serving the relevant applicant with a copy of the request by email, if an email address is listed for the relevant applicant below, or personally or by mail, if a physical address is listed for the relevant applicant below. Hearing requests should be received by the SEC by 5:30 p.m. on December 21, 2021, and should be accompanied by proof of service on applicants, in the form of an affidavit or, for lawyers, a certificate of service. Pursuant to Rule 0–5 under the Act, hearing requests should state the nature of the writer's interest, any facts bearing upon the desirability of a hearing on the matter, the reason for the request, and the issues contested. Persons who wish to be notified of a hearing may request notification by writing to the Commission's Secretary at *Secretarys-Office@sec.gov.*

ADDRESSES: The Commission: *Secretarys-Office@sec.gov.*

FOR FURTHER INFORMATION CONTACT: Shawn Davis, Assistant Director, at (202) 551–6413 or Chief Counsel's Office at (202) 551–6821; SEC, Division of Investment Management, Chief Counsel's Office, 100 F Street NE, Washington, DC 20549–8010.

First Eagle Senior Loan Fund [File No. 811–22874]

Summary: Applicant, a closed-end investment company, seeks an order declaring that it has ceased to be an investment company. On July 16, 2021, and September 17, 2021, applicant made liquidating distributions to its shareholders based on net asset value. Expenses of approximately $872,000 incurred in connection with the liquidation were paid by the applicant. Applicant also has retained $7,836,833 for the purpose of paying outstanding payments to service providers.

Filing Dates: The application was filed on July 21, 2021, and amended on November 15, 2021.

Applicant's Address: andrew.morris@feim.com.

Gabelli Go Anywhere Trust [File No. 811–23035]

Summary: Applicant, a closed-end investment company, seeks an order declaring that it has ceased to be an investment company. On October 28, 2021, applicant made liquidating distributions to its shareholders based on net asset value. Expenses of $21,170 incurred in connection with the liquidation were paid by the applicant. Applicant also has retained $221,497 for the purpose of paying outstanding expenses.

Filing Date: The application was filed on November 10, 2021.

Applicant's Address: Thomas.DeCapo@skadden.com.

Sound Point Floating Rate 2023 Target Term Fund [File No. 811–23119]

Summary: Applicant, a closed-end investment company, seeks an order declaring that it has ceased to be an investment company. Applicant has never made a public offering of its securities and does not propose to make a public offering or engage in business of any kind.

Filing Dates: The application was filed on August 3, 2021, and amended on October 29, 2021.

Applicant's Address: wruberti@soundpointcap.com, mana.behbin@morganlewis.com.

For the Commission, by the Division of Investment Management, pursuant to delegated authority.

J. Matthew DeLesDernier,

Assistant Secretary.

[FR Doc. 2021–26137 Filed 11–30–21; 8:45 am]

BILLING CODE 8011–01–P

DEPARTMENT OF STATE

[Public Notice: 11598]

Designation of Sanaullah Ghafari, Sultan Aziz Azam, and Maulawi Rajab as Specially Designated Global Terrorists

Acting under the authority of and in accordance with section 1(a)(ii)(B) of E.O. 13224 of September 23, 2001, as amended by E.O. 13268 of July 2, 2002, E.O. 13284 of January 23, 2003, and E.O. 13886 of September 9, 2019, I hereby entering the comment submissions into ADAMS.

II. Further Information

The NUREG provides guidance to a licensee for preparing requests for changes of control and about bankruptcy involving byproduct, source, or special nuclear materials licenses. The NUREG also provides the NRC with criteria for reviewing requests for changes of control and bankruptcy. The purpose of this notice is to provide the public with an opportunity to review and provide comments on draft NUREG–1556, Volume 15, Revision 1, ''Consolidated Guidance about Materials Licenses: Guidance about Changes of Control and about Bankruptcy Involving Byproduct, Source, or Special Nuclear Materials Licenses.'' These comments will be considered in the final version or subsequent revisions.

Dated at Rockville, Maryland, this 19th day of March, 2014.

For the U.S. Nuclear Regulatory Commission.

John M. Moses,

Acting Deputy Director, Division of Materials Safety and State Agreements, Office of Federal and State Materials and Environmental Management Programs.

[FR Doc. 2014–06721 Filed 3–25–14; 8:45 am]

BILLING CODE 7590–01–P

NUCLEAR REGULATORY COMMISSION

[NRC–2014–0060]

Response Strategies for Potential Aircraft Threats

AGENCY: Nuclear Regulatory Commission.

ACTION: Regulatory guide; issuance.

SUMMARY: The U.S. Nuclear Regulatory Commission (NRC) is issuing revision 1 to Regulatory Guide (RG) 1.214, ''Response Strategies for Potential Aircraft Threats.'' The revision contains updated references and minor corrections. The revision does not contain substantive changes in the NRC staff's regulatory positions. The guide describes a method that the NRC staff considers acceptable for applicants for, and holders of, nuclear power plant licenses to comply with NRC requirements to develop, implement, and maintain procedures for responding to potential aircraft threats.

ADDRESSES: The document will be made available for those individuals who have established a ''need-to-know'' and possess access permission to Official Use Only-Security Related Information (OUO–SRI). To access and review the document contact: James Vaughn, telephone: 301–287–3586, email: *james.vaughn@nrc.gov.*

FOR FURTHER INFORMATION CONTACT: James Vaughn, telephone: 301–287–3586, email: *james.vaughn@nrc.gov,* or Mekonen Bayssie, telephone: 301–251–7489, email: *mekonen.bayssie@nrc.gov,* U.S. Nuclear Regulatory Commission, Washington, DC 20555–0001.

SUPPLEMENTARY INFORMATION:

I. Introduction

The NRC is issuing a revision to an existing guide in the NRC's ''Regulatory Guide'' series. Regulatory guides were developed to describe and make available to the public, to the extent possible, information and methods that are acceptable to the NRC staff for implementing specific parts of the agency's regulations, techniques that the staff uses in evaluating specific problems or postulated accidents, and data that the staff needs in its review of applications for permits and licenses. The NRC typically seeks public comment on a draft version of a regulatory guide by announcing its availability for comment in the **Federal Register**. However, as explained in section III.F. of the Handbook for NRC Management Directive 6.6, ''Regulatory Guides'' (Agencywide Documents Access and Management System Accession No. ML110330475), the NRC may directly issue a final regulatory guide without a draft version or public comment period if the changes to the regulatory guide are non-substantive. Furthermore, RG 1.214 is withheld from public disclosure but is available to those affected licensees and cleared stakeholders who can or have demonstrated a ''need-to-know.''

The NRC is issuing Revision 1 of RG 1.214 directly as a final regulatory guide because the changes between Revision 0 and Revision 1 are non-substantive. This revision of RG 1.214 incorporates editorial changes, updates the guide to conform to the current format for regulatory guides, and updates references to related guidance for emergency preparedness (EP). These changes are intended to improve clarity of the guidance and alignment with the EP requirements in part 50 of Title 10 of the *Code of Federal Regulations* (10 CFR), Appendix E, and do not alter the staff regulatory guidance.

II. Backfitting and Issue Finality

Issuance of this final regulatory guide does not constitute backfitting as defined in 10 CFR 50.109 (the Backfit Rule) and is not otherwise inconsistent with the issue finality provisions in 10 CFR part 52. The changes in Revision 1 of RG 1.214 are limited to editorial changes to improve clarity of the guidance and alignment with the EP requirements in 10 CFR part 50, Appendix E. These changes do not fall within the kinds of agency actions that constitute backfitting or are subject to limitations in the issue finality provisions of 10 CFR part 52. Accordingly, the NRC did not address the Backfit Rule or issue finality provisions of 10 CFR part 52.

III. Congressional Review Act

This action is not a rule as defined in the Congressional Review Act (5 U.S.C. 801–808).

IV. Submitting Suggestions for Improvement of Regulatory Guides

Revision 1 of RG 1.214 is being issued without an opportunity for comment. However, you may at any time submit suggestions to the NRC for improvement of existing regulatory guides or for the development of new regulatory guides to address new issues. The input received will be considered in future updates and enhancements of the regulatory guide. Please coordinate with James Vaughn from the NRC's Office of Nuclear Security and Incident Response (telephone: 301–287–3686 or email: *james.vaughn@nrc.gov*) regarding the drafting and transmission of such comments in order to protect comments that contain OUO–SRI information.

Dated at Rockville, Maryland, this 19th day of March, 2014.

For the Nuclear Regulatory Commission.

Thomas H. Boyce,

Chief, Regulatory Guide and Generic Issues Branch, Division of Engineering, Office of Nuclear Regulatory Research.

[FR Doc. 2014–06575 Filed 3–25–14; 8:45 am]

BILLING CODE 7590–01–P

OFFICE OF PERSONNEL MANAGEMENT

Privacy Act of 1974: Update and Amend System of Records

AGENCY: U.S. Office of Personnel Management (OPM).

ACTION: Update and amend OPM/GOVT–5, Recruiting, Examining, and Placement Records.

SUMMARY: OPM proposes to update and amend OPM/GOVT–5, Recruiting, Examining, and Placement Records contained in its inventory of record systems subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended. This action is necessary to meet the requirements of the Privacy Act to

OPM-000070

publish in the **Federal Register** notice of the existence and character, as well as any new use or intended new use of records maintained by the agency. 5 U.S.C. 552a(e)(4) and (11).

DATES: These changes will become effective without further notice on May 5, 2014, unless we receive comments that result in a contrary determination.

ADDRESSES: Send written comments to the Director, Integrated Hiring Solutions, Office of the Chief Information Officer, U.S. Office of Personnel Management, 1900 E Street NW., Room 44690, Washington, DC 20415.

FOR FURTHER INFORMATION CONTACT: Paul Craven, Director, Integrated Hiring Solutions, *paul.craven@opm.gov.*

SUPPLEMENTARY INFORMATION: The Office of Personnel Management's (OPM) system of record notices subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended, have been published in the **Federal Register**. The proposed changes consist of the deletion of an OPM office from the System Locations, and the designation of a replacement for the existing System Manager. Both changes reflect the results of an OPM re-organization that eliminated the position previously named as System Manager and the office previously named in the Locations listing.

U.S. Office of Personnel Management.

Katherine Archuleta,

Director.

OPM/GOVT–5

SYSTEM NAME:

Recruiting, Examining, and Placement Records.

SYSTEM LOCATION:

Office of Personnel Management, 1900 E Street NW., Washington, DC 20415, OPM regional and area offices; and personnel or other designated offices of Federal agencies that are authorized to make appointments and to act for the Office by delegated authority.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

a. Persons who have applied to the Office or agencies for Federal employment and current and former Federal employees submitting applications for other positions in the Federal service.

b. Applicants for Federal employment believed or found to be unsuitable for employment on medical grounds.

CATEGORIES OF RECORDS IN THE SYSTEM:

In general, all records in this system contain identifying information including name, date of birth, Social Security Number, and home address. These records pertain to assembled and unassembled examining procedures and contain information on both competitive examinations and on certain noncompetitive actions, such as determinations of time-in-grade restriction waivers, waiver of qualification requirement determinations, and variations in regulatory requirements in individual cases.

This system includes such records as:

a. Applications for employment that contain information on work and education, military service, convictions for offenses against the law, military service, and indications of specialized training or receipt of awards or honors. These records may also include copies of correspondence between the applicant and the Office or agency.

b. Results of written exams and indications of how information in the application was rated. These records also contain information on the ranking of an applicant, his or her placement on a list of eligibles, what certificates applicant's names appeared on, an agency's request for Office approval of the agency's objection to an eligible's qualifications and the Office's decision in the matter, an agency's request for Office approval for the agency to pass over an eligible and the Office's decision in the matter, and an agency's decision to object/pass over an eligible when the agency has authority to make such decisions under agreement with the Office.

c. Records regarding the Office's final decision on an agency's decision to object/pass over an eligible for suitability or medical reasons or when the objection/pass over decision applies to a compensable preference eligible with 30 percent or more disability. (Does not include a rating of ineligibility for employment because of a confirmed positive test result under Executive Order 12564.)

d. Responses to and results of approved personality or similar tests administered by the Office or agency.

e. Records relating to rating appeals filed with the Office or agency.

f. Registration sheets, control cards, and related documents regarding Federal employees requesting placement assistance in view of pending or realized displacement because of reduction in force, transfer or discontinuance of function, or reorganization.

g. Records concerning non-competitive action cases referred to the Office for decision. These files include such records as waiver of time-in-grade requirements, decisions on superior qualification appointments, temporary appointments outside a register, and employee status determinations. Authority for making decisions on many of these actions has also been delegated to agencies. The records retained by the Office on such actions and copies of such files retained by the agency submitting the request to the Office, along with records that agencies maintain as a result of the Office's delegations of authorities, are considered part of this system of records.

h. Records retained to support Schedule A appointments of severely physically handicapped individuals, retained both by the Office and agencies acting under the Office delegated authorities, are part of this system.

i. Agency applicant supply file systems (when the agency retains applications, resumes, and other related records for hard-to-fill or unique positions, for future consideration), along with any pre-employment vouchers obtained in connection with an agency's processing of an application, are included in this system.

j. Records derived from the Office-developed or agency-developed assessment center exercises.

k. Case files related to medical suitability determinations and appeals.

l. Records related to an applicant's examination for use of illegal drugs under provisions of Executive Order 12564. Such records may be retained by the agency (e.g., evidence of confirmed positive test results) or by a contractor laboratory (e.g., the record of the testing of an applicant, whether negative, or confirmed or unconfirmed positive test result).

NOTE 1:

Only Routine Use 'p' identified for this system of records is applicable to records relating to drug testing under Executive Order 12564. Further, such records shall be disclosed only to a very limited number of officials within the agency, generally only to the agency Medical Review Official (MRO), the administrator of the agency Employee Assistance Program, and any supervisory or management official within the employee's agency having authority to take the adverse personnel action against the employee.

NOTE 2:

OPM does not intend that records created by agencies in connection with the agency's Merit Promotion Plan program be included in the term 'Applicant Supply File' as used within this notice. It is OPM's position that

Merit Promotion Plan records are not a system of records within the meaning of the Privacy Act as such records are usually filed by a vacancy announcement number or some other key that is not a unique personnel identifier. Agencies may choose to consider such records as within the meaning of a system of records as used in the Privacy Act, but if they do so, they are solely responsible for implementing Privacy Act requirements, including establishment and notice of a system of records pertaining to such records.

NOTE 3:

To the extent that an agency utilizes an automated medium in connection with maintenance of records in this system, the automated versions of these records are considered covered by this system of records.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 1302, 3109, 3301, 3302, 3304, 3305, 3306, 3307, 309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533, and Executive Order 9397.

PURPOSE(S):

The records are used in considering individuals who have applied for positions in the Federal service by making determinations of qualifications including medical qualifications, for positions applied for, and to rate and rank applicants applying for the same or similar positions. They are also used to refer candidates to Federal agencies for employment consideration, including appointment, transfer, reinstatement, reassignment, or promotion. Records derived from the Office-developed or agency-developed assessment center exercises may be used to determine training needs of participants. These records may also be used to locate individuals for personnel research.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSE OF SUCH USES:

NOTE 4:

With the exception of Routine Use 'p,' none of the Other Routine Uses identified for this system of records are applicable to records relating to drug testing under Executive Order 12564. Further, such records shall be disclosed only to a very limited number of officials within that agency, generally only to the agency Medical Review Officer (MRO), the administrator of the agency's Employee Assistance Program, and the management official empowered to recommend or take adverse action affecting the individual.

a. To refer applicants, including current and former Federal employees to Federal agencies for consideration for employment, transfer, reassignment, reinstatement, or promotion.

b. With the permission of the applicant, to refer applicants to State and local governments, congressional offices, international organizations, and other public offices for employment consideration.

c. To disclose pertinent information to the appropriate Federal, State, or local agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, when the disclosing agency becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation.

d. To disclose information to any source from which additional information is requested (to the extent necessary to identify the individual, inform the source of the purposes of the request, and to identify the type of information requested), when necessary to obtain information relevant to an agency decision concerning hiring or retaining an employee, issuing a security clearance, conducting a security or suitability investigation of an individual, classifying positions, letting a contract, or issuing a license, grant or other benefit.

e. To disclose information to a Federal agency, in response to its request, in connection with hiring or retaining an employee, issuing a security clearance, conducting a security or suitability investigation of an individual, classifying positions, letting a contract, or issuing a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision in the matter.

f. To disclose information to the Office of Management and Budget at any stage in the legislative coordination and clearance process in connection with private relief legislation as set forth in OMB Circular No. A–19.

g. To provide information to a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of that individual.

h. To disclose information to another Federal agency, to a court, or a party in litigation before a court or in an administrative proceeding being conducted by a Federal agency, when the Government is a party to a judicial or administrative proceeding.

i. To disclose information to the Department of Justice, or in a proceeding before a court, adjudicative body, or other administrative body before which the agency is authorized to appear, when:

1. The agency, or any component thereof; or

2. Any employee of the agency in his or her official capacity; or

3. Any employee of the agency in his or her individual capacity where the Department of Justice or the agency has agreed to represent the employee; or

4. The United States, when the agency determines that litigation is likely to affect the agency or any of its components, is a party to litigation or has an interest in such litigation, and the use of such records by the Department of Justice or the agency is deemed by the agency to be relevant and necessary to the litigation, provided, however, that in each case it has been determined that the disclosure is compatible with the purpose for which the records were collected.

j. By the National Archives and Records Administration in records management inspections and its role as Archivist.

k. By the agency maintaining the records or by the Office to locate individuals for personnel research or survey response or in producing summary descriptive statistics and analytical studies in support of the function for which the records are collected and maintained, or for related workforce studies. While published statistics and studies do not contain individual identifiers, in some instances the selection of elements of data included in the study may be structured in such a way as to make the data individually identifiable by inference.

l. To disclose information to the Merit Systems Protection Board or the Office of the Special Counsel in connection with appeals, special studies of the civil service and other merit systems, review of Office rules and rules and regulations, investigations of alleged or possible prohibited personnel practices, and such other functions; e.g., as prescribed in 5 U.S.C. chapter 12, or as may be authorized by law.

m. To disclose information to the Equal Employment Opportunity Commission when requested in connection with investigations into alleged or possible discrimination practices in the Federal sector, examination of Federal affirmative employment programs, compliance by Federal agencies with the Uniform Guidelines or Employee Selection Procedures, or other functions vested in the Commission.

n. To disclose information to the Federal Labor Relations Authority or its General Counsel when requested in connection with investigations of allegations of unfair labor practices or matters before the Federal Service Impasses Panel.

o. To disclose, in response to a request for discovery or for an appearance of a witness, information that is relevant to the subject matter involved in a pending judicial or administrative proceeding.

p. To disclose the results of a drug test of a Federal employee pursuant to an order of a court of competent jurisdiction where required by the United States Government to defend against any challenge against any adverse personnel action.

q. To disclose information to Federal, State, local, and professional licensing boards, Boards of Medical Examiners, or to the Federation of State Medical Boards or a similar non-government entity which maintains records concerning the issuance, retention, or revocation of licenses, certifications, or registration necessary to practice an occupation, profession, or specialty, in order to obtain information relevant to an agency decision concerning the hiring, retention, or termination of an employee or to inform a Federal agency or licensing board or the appropriate non-government entity about the health care practice of a terminated, resigned, or retired health care employee whose professional health care activity so significantly failed to conform to generally accepted standards of professional medical practice as to raise reasonable concern for the health and safety of patients in the private sector or from another Federal agency.

r. To disclose information to contractors, grantees, or volunteers performing or working on a contract, service, grant, cooperative agreement, or job for the Federal Government.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, SAFEGUARDING, RETAINING AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records are maintained on magnetic tapes, disk, punched cards, microfiche, cards, lists, and forms.

RETRIEVABILITY:

Records are retrieved by the name, date of birth, social security number, and/or identification number assigned to the individual on whom they are maintained.

SAFEGUARDS:

Records are maintained in a secured area or automated media with access limited to authorized personnel whose duties require access.

RETENTION AND DISPOSAL:

Records in this system are retained for varying lengths of time, ranging from a few months to 5 years, e.g., applicant records that are part of medical determination case files or medical suitability appeal files are retained for 3 years from completion of action on the case. Most records are retained for a period of 1 to 2 years. Some records, such as individual applications, become part of the person's permanent official records when hired, while some records (e.g., non-competitive action case files), are retained for 5 years. Some records are destroyed by shredding or burning while magnetic tapes or disks are erased.

SYSTEM MANAGER(S) AND ADDRESS:

Director, Integrated Hiring Solutions, Office of the Chief Information Officer, U.S. Office of Personnel Management, 1900 E Street NW., Room 44690, Washington, DC 20415.

NOTIFICATION PROCEDURE:

Individuals wishing to inquire whether this system of records contains information about them should contact the agency or OPM where application was made or examination was taken. Individuals must provide the following information for their records to be located and identified:

a. Name.
b. Date of birth.
c. Social Security Number.
d. Identification number (if known).
e. Approximate date of record.
f. Title of examination or announcement with which concerned.
g. Geographic area in which consideration was requested.

RECORD ACCESS PROCEDURE:

Specific materials in this system have been exempted from Privacy Act provisions at 5 U.S.C. (c)(3) and (d), regarding access to records.

The section of this notice titled ''Systems Exempted from Certain Provisions of the Act'' indicates the kind of material exempted and the reasons for exempting them from access. Individuals wishing to request access to their non-exempt records should contact the agency or the OPM where application was made or examination was taken. Individuals must provide the following information for their records to be located and identified:

a. Name.
b. Date of birth.
c. Social Security Number.
d. Identification number (if known).
e. Approximate date of record.
f. Title of examination or announcement with which concerned.
g. Geographic area in which consideration was requested.

Individuals requesting access must also comply with the OPM's Privacy Act regulations on verification of identity and access to records (5 CFR part 297).

CONTESTING RECORD PROCEDURE:

Specific materials in this system have been exempted from Privacy Act provisions at 5 U.S.C. 552a(d), regarding amendment of records. The section of this notice titled 'Systems Exempted from Certain Provisions of the Act' indicates the kinds of material exempted and the reasons for exempting them from amendment. An individual may contact the agency or the Office where the application is filed at any time to update qualifications, education, experience, or other data maintained in the system.

Such regular administrative updating of records should not be requested under the provisions of the Privacy Act. However, individuals wishing to request amendment of other records under the provisions of the Privacy Act should contact the agency or the OPM where the application was made or the examination was taken. Individuals must provide the following information for their records to be located and identified:

a. Name.
b. Date of birth.
c. Social Security Number.
d. Identification number (if known).
e. Approximate date of record.
f. Title of examination or announcement with which concerned.
g. Geographic area in which consideration was requested.

Individuals requesting amendment must also comply with the OPM's Privacy Act regulations on verification of identity and amendment of records (5 CFR part 297).

NOTE 5:

In responding to an inquiry or a request for access or amendment, resource specialists may contact the OPM's area office that provides examining and rating assistance for help in processing the request.

RECORD SOURCE CATEGORIES:

Information in this system of records comes from the individual to whom it applies or is derived from information the individual supplied, reports from medical personnel on physical qualifications, results of examinations that are made known to applicants, agencies, and OPM records, and vouchers supplied by references or other sources that the applicant lists or that are developed.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

This system contains investigative materials that are used solely to determine the appropriateness of a request for approval of an objection to an eligible's qualifications for Federal civilian employment or vouchers received during the processing of an application. The Privacy Act, at 5 U.S.C. 552a(k)(5), permits an agency to exempt such investigative material from certain provisions of the Act, to the extent that release of the material to the individual whom the information is about would—

a. Reveal the identity of a source who furnished information to the Government under an express promise (granted on or after September 27, 1975) that the identity of the source would be held in confidence; or

b. Reveal the identity of a source who, prior to September 27, 1975, furnished information to the Government under an implied promise that the identity of the source would be held in confidence.

This system contains testing and examination materials used solely to determine individual qualifications for appointment or promotion in the Federal service. The Privacy Act, at 5 U.S.C. 552a(k)(6), permits an agency to exempt all such testing or examination material and information from certain provisions of the Act, when disclosure of the material would compromise the objectivity or fairness of the testing or examination process. OPM has claimed exemptions from the requirements of 5 U.S.C. 552a(d), which relate to access to and amendment of records.

The specific material exempted include, but are not limited to, the following

a. Answer keys.

b. Assessment center exercises.

c. Assessment center exercise reports.

d. Assessor guidance material.

e. Assessment center observation reports.

f. Assessment center summary reports.

g. Other applicant appraisal methods, such as performance tests, work samples and simulations, miniature training and evaluation exercises, structured interviews, and their associated evaluation guides and reports.

h. Item analyses and similar data that contain test keys and item response data.

i. Ratings given for validating examinations.

j. Rating schedules, including crediting plans and scoring formulas for other selection procedures.

k. Rating sheets.

l. Test booklets, including the written instructions for their preparation and automated versions of tests and related selection materials and their complete documentation.

m. Test item files.

n. Test answer sheets.

[FR Doc. 2014–06593 Filed 3–25–14; 8:45 am]

BILLING CODE 6325–39–P

POSTAL SERVICE

Board of Governors; Sunshine Act Meeting

DATES AND TIMES: April 8, 2014, at 9:00 a.m.

PLACE: Washington, DC.

STATUS: Closed.

MATTERS TO BE CONSIDERED:

Tuesday, April 8, 2014 at 9:00 a.m.

1. Strategic Issues.
2. Financial Matters.
3. Pricing.
4. Personnel Matters and Compensation Issues.
5. Governors' Executive Session—Discussion of prior agenda items and Board Governance.

CONTACT PERSON FOR MORE INFORMATION: Julie S. Moore, Secretary of the Board, U.S. Postal Service, 475 L'Enfant Plaza SW., Washington, DC 20260–1000. Telephone (202) 268–4800.

Julie S. Moore,

Secretary.

[FR Doc. 2014–06862 Filed 3–24–14; 4:15 pm]

BILLING CODE 7710–12–P

SECURITIES AND EXCHANGE COMMISSION

[OMB Control No. 3235–0515, SEC File No. 270–456]

Submission for OMB Review; Comment Request

Upon Written Request Copies Available From: Securities and Exchange Commission, Office of Investor Education and Advocacy, Washington, DC 20549–0213.

Extension:
Schedule TO.

Notice is hereby given that, pursuant to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*), the Securities and Exchange Commission (''Commission'') has submitted to the Office of Management and Budget the request for extension of the previously approved collection of information discussed below.

Schedule TO (17 CFR 240.14d–100) must be filed by a reporting company that makes a tender offer for its own securities. Also, persons other than the reporting company making a tender offer for equity securities registered under Section 12 of the Exchange Act (15 U.S.C. 78*l*) (which offer, if consummated, would cause that person to own over 5% of that class of the securities) must file a Schedule TO. The purpose of Schedule TO is to improve communications between public companies and investors before companies file registration statements involving tender offer statements. This information is made available to the public. The information provided on Schedule TO is mandatory. Schedule TO takes approximately 43.5 hours per response and is filed by approximately 820 issuers annually. We estimate that 50% of the 43.5 hours per response (21.75 hours) is prepared by the issuer for an annual reporting burden of 17,835 hours (21.75 hours per response × 820 responses).

An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid control number.

The public may view the background documentation for this information collection at the following Web site, *www.reginfo.gov* . Comments should be directed to: (i) Desk Officer for the Securities and Exchange Commission, Office of Information and Regulatory Affairs, Office of Management and Budget, Room 10102, New Executive Office Building, Washington, DC 20503, or by sending an email to: *Shagufta_Ahmed@omb.eop.gov;* and (ii) Thomas Bayer, Director/Chief Information Officer, Securities and Exchange Commission, c/o Remi Pavlik-Simon, 100 F Street NE., Washington, DC 20549 or send an email to: *PRA_Mailbox@sec.gov.* Comments must be submitted to OMB within 30 days of this notice.

Dated: March 20, 2014.

Kevin M. O'Neill,

Deputy Secretary.

[FR Doc. 2014–06609 Filed 3–25–14; 8:45 am]

BILLING CODE 8011–01–P

SECURITIES AND EXCHANGE COMMISSION

Submission for OMB Review; Comment Request

Upon Written Request, Copies Available From: Securities and Exchange Commission, Office of Investor Education and Advocacy, Washington, DC 20549–0213.

Extension:
Rule 15b6–1 and Form BDW, SEC File No. 270–17, OMB Control No. 3235–0018.

Notice is hereby given that, pursuant to the Paperwork Reduction Act of 1995

Account Creation Audit Between 1/20/25 - 2/12/2025

Employee Name	Account Username	System Name	Date Created	Date Removed	Admin Access	Login Yes/No
[OPM-3]	\mcn\app\MGA\Users\[OPM-3]	APP.mcn Domain	1/20/20253:46:12 PM			
[OPM-3]	[OPM-3]@opm.gov	Azure DevOps	1/21/2025			
[OPM-3]	\mcn\cld\MGA\Users\[OPM-3]	CLD.mcn Domain	1/20/20253:38:26 PM			
[OPM-3]	[OPM-3]@opm.gov	OPM Data : Connect Platform (Az.opm.entraID.efficiencyorg.admin + Az.cio.entraID.PowerBIAdmin)	1/20/2025			
[OPM-3]	[OPM-3]@opm.gov	USA Staffing Core + Admin Portal - DEV/TST/STG/TRN/PRD	1/20/2025			
[OPM-3]	[OPM-3]@opm.gov	Web Admin	1/20/2025			
[OPM-16]	[OPM-16]@opm.gov	USA Performance - Office of the Director	1/31/2025			
Amanda Scale	\mcn\cld\MGA\Users\Amanda Scale	CLD.mcn Domain	1/20/20253:30:19 PM			
Amanda Scales	amanda.scales@opm.gov	Agency Talent Portal	1/21/2025			
Amanda Scales	\mcn\app\MGA\Users\Amanda Scales	APP.mcn Domain	1/20/20253:43:44 PM			
Amanda Scales	\mcn\cld\MGA\Users\Amanda Scales	CLD.mcn Domain	1/20/20254:30:19 PM			
Amanda Scales	adscales@opm.gov	OD Reports : New Hire Daily Tracker Power BI - USADATA	1/31/2025			
Amanda Scales	adscales@opm.gov	OPM Data : Azure Databricks Admin + NP / PRD Azure Subscriptions [OPMData / USADATA]	2/3/2025			
Amanda Scales	amanda.scales@opm.gov	USA Staffing Core + Admin Portal - DEV/TST/STG/TRN/PRD	1/20/2025			
Amanda Scales	Amanda.Scales@opm.gov	Web Admin	1/20/2025			
[PII]	[PII]	ESCS	2/11/2025			
[OPM-9]	[OPM-9]@opm.gov	OD Reports : New Hire Daily Tracker Power BI - USADATA	2/4/2025			
[OPM-9]	[OPM-9]@opm.gov	OPM Data : Azure Databricks Admin + NP / PRD Azure Subscriptions [OPMData / USADATA]	2/4/2025			
[OPM-9]	[OPM-9]@opm.gov	USA Performance - Office of the Director	1/31/2025			
[OPM-2]	[OPM-2]_opmgov	GitHub Enterprise	1/28/2025			
[OPM-7]	[OPM-7]_opmgov	GitHub Enterprise	1/20/2025			
[OPM-7]	[OPM-7]@opm.gov	USA Performance - U.S. Office of Personnel Management	1/20/2025			
[OPM-3]	[OPM-3]_opmgov	GitHub Enterprise	1/20/2025			
[OPM-3]	[OPM-3]@opm.gov	USA Performance - U.S. Office of Personnel Management	1/20/2025			
[PII]	[PII]	USA Performance - Office of the Director	1/31/2025			
[PII]	[PII]	STAMP	1/27/2025			
[OPM-7]	\mcn\app\MGA\Users\[OPM-7]	APP.mcn Domain	1/20/20253:45:37 PM			
[OPM-7]	\mcn\cld\MGA\Users\[OPM-7]	CLD.mcn Domain	1/20/20253:37:48 PM			
[OPM-7]	[OPM-7]@opm.gov	USA Staffing Core + Admin Portal - DEV/TST/STG/TRN/PRD	1/20/2025			
[OPM-7]	[OPM-7]@opm.gov	Web Admin	1/20/2025			
Charles Ezell	\mcn\app\MGA\Users\Charles Ezell	APP.mcn Domain	1/20/20253:46:34 PM			
Charles Ezell	\mcn\cld\MGA\Users\Charles Ezell	CLD.mcn Domain	1/20/20253:41:54 PM			
Charles Ezell	charles.ezell@opm.gov	OPM Data : Connect Platform (Az.opm.entraID.efficiencyorg.admin + Az.cio.entraID.PowerBIAdmin)	1/20/2025			
Charles Ezell	charles.ezell@opm.gov	USA Staffing Core + Admin Portal - DEV/TST/STG/TRN/PRD	1/20/2025			
Charles Ezell	Charles.Ezell@opm.gov	Web Admin	1/20/2025			
[PII]	[PII]	Postal Reform	1/27/2025			
[PII]	[PII]	DFS	1/22/2025			
[PII]	[PII]	ARS (DCCS)	2/5/2025			
[PII]	[PII]	ARS (DCCS)	2/6/2025			
[PII]	[PII]	ARS (AVAS)	1/21/2025			
[PII]	[PII]	ARS (AVAS)	1/21/2025			
[PII]	[PII]	ARS (AVAS)	1/21/2025			
[PII]	[PII]	ARS (AVAS)	1/22/2025			
[PII]	[PII]	ARS (AVAS)	1/23/2025			
[PII]	[PII]	BFMS (FMCD 2812)	1/22/2025			
[PII]	(HB Carrier - RACF IDs)	BFMS (FMCD 2812)	1/22/2025			
[PII]	(HB Carrier - RACF IDs)	BFMS (FMCD 2812)	1/22/2025			
[PII]	(HB Carrier - RACF IDs)	BFMS (FMCD 2812)	1/22/2025			
[PII]	(HB Carrier - RACF IDs)	BFMS (FMCD 2812)	1/23/2025			
[PII]	(HB Carrier - RACF IDs)	BFMS (FMCD 2812)	1/23/2025			
[PII]	(HB Carrier - RACF IDs)	BFMS (FMCD 2812)	1/23/2025			
[PII]	(HB Carrier - RACF IDs)	BFMS (FMCD 2812)	1/23/2025			
[PII]	[PII]	BFMS (FMCD 2812)	1/23/2025			
[PII]	(HB Carrier - RACF IDs)	BFMS (FMCD 2812)	1/23/2025			
[PII]	(HB Carrier - RACF IDs)	BFMS (FMCD 2812)	1/23/2025			
[PII]	(HB Carrier - RACF IDs)	BFMS (FMCD 2812)	1/24/2025			
[PII]	(HB Carrier - RACF IDs)	BFMS (FMCD 2812)	1/28/2025			
[PII]	(HB Carrier - RACF IDs)	BFMS (FMCD 2812)	1/28/2025			
[PII]	(HB Carrier - RACF IDs)	BFMS (FMCD 2812)	1/28/2025			
[PII]	[PII]	ARS (DCCS)	1/31/2025			
[PII]	[PII]	ARS (AVAS)	2/6/2025			
[PII]	[PII]	ARS (DCCS)	2/10/2025			
[PII]	[PII]	ARS (DCCS)	2/10/2025			
[PII]	[PII]	ARS (DCCS)	2/10/2025			
[PII]	[PII]	ARS (DCCS)	2/10/2025			
[PII]	[PII]	CIITAR	1/21/2025			
[PII]	[PII]	CIITAR	1/21/2025			
[PII]	[PII]	CIITAR	1/30/2025			
[PII]	[PII]	CIITAR	2/12/2025			
[PII]	[PII]	USA Performance - CFO - Budget	1/24/2025			
[PII]	[PII]	USA Performance - CFO - Budget	1/24/2025			
[PII]	[PII]	USA Performance - CFO - Budget	1/24/2025			
[PII]	[PII]	USA Performance - CFO - Budget	1/24/2025			
[PII]	[PII]	USA Performance - CFO - Chief Financial Officer	1/24/2025			
[PII]	[PII]	USA Performance - CIO - Chief Technology Officer	1/24/2025			
[PII]	[PII]	USA Performance - CIO - Chief Technology Officer	1/24/2025			
[PII]	[PII]	USA Performance - CIO - FITBS - Hiring Systems	1/24/2025			
[PII]	[PII]	USA Performance - CIO - FITBS - HR Solutions IT PMO	1/24/2025			
[PII]	[PII]	USA Performance - CIO - FITBS - Recruitment Systems	1/24/2025			
[PII]	[PII]	USA Performance - CIO - FITBS - Recruitment Systems	1/24/2025			
[PII]	[PII]	USA Performance - CIO - FITBS - Recruitment Systems	1/24/2025			
[PII]	[PII]	USA Performance - CIO - FITBS - Systems Capacity	1/24/2025			
[PII]	[PII]	USA Performance - CIO - FITBS - Systems Capacity	1/24/2025			
[PII]	[PII]	USA Performance - CIO - FITBS - Systems Capacity	1/24/2025			
[PII]	[PII]	USA Performance - CIO - ITS - IT Security Management	1/24/2025			
[PII]	[PII]	USA Performance - CIO - ITS - Security Operations Center	1/24/2025			
[PII]	[PII]	USA Performance - CIO - RM - Resource Management	1/24/2025			
[PII]	[PII]	USA Performance - FSEM - Facilities, Security & Emergency Mgmt - Emergency Management	1/24/2025			
[PII]	[PII]	USA Performance - HCDMM - Human Capital Data Management & Moderniz - Data Support and Analysis	1/24/2025			
[PII]	[PII]	USA Performance - HI - Healthcare & Insurance - Actuaries	1/24/2025			
[PII]	[PII]	USA Performance - HI - Healthcare & Insurance - Actuaries	1/24/2025			
[PII]	[PII]	USA Performance - HI - Healthcare & Insurance - Audit Resolution & Compliance	1/24/2025			
[PII]	[PII]	USA Performance - HI - Healthcare & Insurance - Disputed Claims	1/24/2025			
[PII]	[PII]	USA Performance - HI - Healthcare & Insurance - Disputed Claims	1/24/2025			
[PII]	[PII]	USA Performance - HI - Healthcare & Insurance - Disputed Claims	1/24/2025			
[PII]	[PII]	USA Performance - HI - Healthcare & Insurance - FEHB 3	1/24/2025			
[PII]	[PII]	USA Performance - HI - Healthcare & Insurance - Life and Ancillary Benefits	1/24/2025			
[PII]	[PII]	USA Performance - HI - Healthcare & Insurance - Operations and Resource Management	2/7/2025			
[PII]	[PII]	USA Performance - HI - Healthcare & Insurance - Program Analysis & Development	1/24/2025			
[PII]	[PII]	USA Performance - HI - Healthcare and Insurance	1/24/2025			
[PII]	[PII]	USA Performance - HI - PSIO 1	1/24/2025			
[PII]	[PII]	USA Performance - HRS - Applied Analytics Branch	1/24/2025			
[PII]	[PII]	USA Performance - HRS - Enterprise Leadership Solutions	1/24/2025			

Employee Name	Account Username	System Name	Date Created	Date Removed	Admin Access	Login Yes/No
[PII]	[PII]	USA Performance - HRS - Federal Classification Center	1/31/2025			
[PII]	[PII]	USA Performance - MSAC - ACE Western	1/24/2025			
[PII]	[PII]	USA Performance - MSAC - Merit System Accountability and Compliance	1/24/2025			
[PII]	[PII]	USA Performance - OCHCO - Executive Resources	1/24/2025			
[PII]	[PII]	USA Performance - OCHCO - Talent Acquisition A	1/24/2025			
[PII]	[PII]	USA Performance - OCR - Office of Civil Rights	1/24/2025			
[OPM-4]	[OPM-4]@opm.gov	USA Performance - U.S. Office of Personnel Management	1/28/2025			
[PII]	[PII]	USA Performance - Office of Communications	1/24/2025			
[PII]	[PII]	USA Performance - Office of Exec Sec & Privacy & Info Management	1/31/2025			
[PII]	[PII]	USA Performance - Office of Exec Sec & Privacy & Info Management	2/7/2025			
[PII]	[PII]	USA Performance - Office of Exec Sec & Privacy & Info Management	1/24/2025			
[PII]	[PII]	STAMP	1/31/2025			
[PII]	[PII]	USA Performance - OGC - General Counsel	1/31/2025			
[OPM-15]	[OPM-15]@opm.gov	USA Performance - Office of the Director	2/7/2025			
[OPM-4]	\mcn\cld\MGA\Users\[OPM-4]	CLD.mcn Domain	1/28/202511:39:49 AM			
[OPM-12]	[OPM-12]@opm.gov	USA Performance - Office of the Director	2/7/2025			
[OPM-11]	[OPM-11]@opm.gov	USA Performance - Office of the Director	2/7/2025			
[OPM-4]	[OPM-6]@opm.gov	OPM Data : Azure Databricks Admin + NP / PRD Azure Subscriptions [OPMData / USADATA]	1/28/2025			
[OPM-4]	[OPM-6]@opm.gov	OPM Data : Connect Platform (Az.opm.entraID.efficiencyorg.admin + Az.cio.entraID.PowerBIAdmin)	1/28/2025			
[OPM-4]	[OPM-6]@opm.gov	OPM Data : Electronic Official Personnel Folder (eOPF) - DEV/TST/QA/TRN/PRD	1/28/2025	2/6/2025		
[OPM-4]	[OPM-6]@opm.gov	OPM Data : Enterprise Human Resources Integration (EHRI) - Dev/TST/QA/PRD	1/28/2025	2/6/2025		
[OPM-4]	[OPM-6]@opm.gov	USA Staffing Core + Admin Portal - DEV/TST/STG/TRN/PRD	1/28/2025			
[OPM-4]	[OPM-6]@opm.gov	Web Admin	1/28/2025			
[OPM-14]	[OPM-14]@opm.gov	USA Performance - Office of the Director	2/7/2025			
[PII]	[PII]	USA Performance - OGC - Comp, Ben, Prod & Svcs	1/24/2025			
Ezell, Charles E.	Charles.Ezell@opm.gov	STAMP	1/23/2025			
[PII]	[PII]	USA Performance - OGC - Merit Sys & Accountability	1/24/2025			
[PII]	[PII]	USA Performance - OIG - Information Sys Audits Grp	1/24/2025			
[PII]	[PII]	USA Performance - OSI - Office of Strategy and Innovation (OSI)	1/24/2025			
[PII]	[PII]	USA Performance - RS - Branch 1	1/24/2025			
[PII]	[PII]	USA Performance - RS - Branch 1	1/24/2025			
[PII]	[PII]	USA Performance - RS - Branch 1	1/24/2025			
[PII]	[PII]	USA Performance - RS - Branch 2	1/24/2025			
[PII]	[PII]	USA Performance - RS - Branch 3	1/24/2025			
[PII]	[PII]	USA Performance - RS - Branch 3	1/24/2025			
[PII]	[PII]	USA Performance - RS - Branch 3	1/24/2025			
[PII]	[PII]	USA Performance - RS - Imaging/Central	1/24/2025			
[PII]	[PII]	USA Performance - RS - Retirement Benefits	1/24/2025			
[PII]	[PII]	USA Performance - RS - Retirement Claims 6	1/24/2025			
[PII]	[PII]	USA Performance - RS - Retirement Services System Support	1/24/2025			
[PII]	[PII]	USA Performance - RS - RIO 10	1/24/2025			
[PII]	[PII]	USA Performance - RS - RIO 6	1/24/2025			
[PII]	[PII]	USA Performance - RS - RIO 7	1/24/2025			
[PII]	[PII]	USA Performance - SuitEA - Policy & Strategy	1/24/2025			
[PII]	[PII]	USA Performance - SuitEA - Policy & Strategy	1/24/2025			
[OPM-5]	\mcn\app\MGA\Users\[OPM-5]	APP.mcn Domain	1/20/20253:44:47 PM			
[OPM-5]	\mcn\cld\MGA\Users\[OPM-5]	CLD.mcn Domain	1/20/20253:35:33 PM			
[OPM-5]	[OPM-5]@opm.gov	OPM Data : Azure Databricks Admin + NP / PRD Azure Subscriptions [OPMData / USADATA]	1/28/2025			
[OPM-5]	[OPM-5]@opm.gov	OPM Data : Connect Platform (Az.opm.entraID.efficiencyorg.admin + Az.cio.entraID.PowerBIAdmin)	1/20/2025			
[OPM-5]	[OPM-5]@opm.gov	USA Staffing Core + Admin Portal - DEV/TST/STG/TRN/PRD	1/20/2025			
[OPM-5]	[OPM-5]@opm.gov	Web Admin	1/20/2025			
Greg Hogan	\mcn\app\MGA\Users\Greg Hogan	APP.mcn Domain	1/20/20253:45:12 PM			
Greg Hogan	Greg.Hogan@opm.gov	Azure DevOps	1/27/2025			
[PII]	[PII]	USA Performance - WPI - Central Region	1/24/2025			
[PII]	[PII]	USA Performance - WPI - Central Region	2/7/2025			
[PII]	[PII]	USA Performance - WPI - FEB - Field Operations	1/24/2025			
[PII]	[PII]	USA Performance - WPI - Forecasting and Methods	1/24/2025			
[PII]	[PII]	USA Performance - WPI - Hiring Policy (Staffing)	2/7/2025			
[PII]	[PII]	USA Performance - WPI - Resource Mgmt Grp	1/23/2025			
[PII]	[PII]	USA Performance - WPI - Western Region	1/24/2025			
Greg Hogan	\mcn\cld\MGA\Users\Greg Hogan	CLD.mcn Domain	1/20/20253:36:46 PM			
[PII]	[PII]	Agency Talent Portal	1/24/2025			
Greg Hogan	Greg.Hogan@opm.gov	ITSP Project Intake app	1/27/2025			
Greg Hogan	Greg.Hogan@opm365.onmicrosoft.com	ITSP Project Intake app	2/6/2025			
Greg Hogan	greg.hogan@opm.gov	OPM Data : Azure Databricks Admin + NP / PRD Azure Subscriptions [OPMData / USADATA]	1/28/2025			
Greg Hogan	greg.hogan@opm.gov	OPM Data : Connect Platform (Az.opm.entraID.efficiencyorg.admin + Az.cio.entraID.PowerBIAdmin)	1/20/2025			
Greg Hogan	greg.hogan@opm.gov	USA Staffing Core + Admin Portal - DEV/TST/STG/TRN/PRD	1/20/2025			
Greg Hogan	Greg.Hogan@opm.gov	Web Admin	1/20/2025			
Hogan, Greg	Greg-Hogan_opmgov	GitHub Enterprise	1/20/2025			
Hogan,Greg	Greg.Hogan@opm.gov	USA Performance - U.S. Office of Personnel Management	1/20/2025			
[OPM-8]	[OPM-8]@opm.gov	OD Reports : New Hire Daily Tracker Power BI - USADATA	2/2/2025			
[OPM-8]	[OPM-8]@opm.gov	OPM Data : Azure Databricks Admin + NP / PRD Azure Subscriptions [OPMData / USADATA]	2/3/2025			
[OPM-8]	[OPM-8]@opm.gov	USA Staffing Core + Admin Portal - DEV/TST/STG/TRN/PRD	2/3/2025			
[OPM-5]	[OPM-5]_opmgov	GitHub Enterprise	1/20/2025			
[OPM-5]	[OPM-5]@opm.gov	USA Performance - U.S. Office of Personnel Management	1/20/2025			
[PII]	[PII]	STAMP	1/31/2025			
[PII]	[PII]	CLD.mcn Domain	1/21/20253:10:22 PM			
[PII]	[PII]	APP.mcn Domain	1/22/20258:36:39 AM			
[PII]	[PII]	APP.mcn Domain	1/22/20258:38:57 AM			
[PII]	[PII]	CLD.mcn Domain	1/22/20258:40:16 AM			
[PII]	[PII]	CLD.mcn Domain	1/22/20258:41:06 AM			
[OPM-17]	[OPM-17]@opm.gov	USA Performance - Office of the Director	1/31/2025			
[OPM-6]	[OPM-6]@opm.gov	Agency Talent Portal	1/31/2025			
[OPM-6]	\mcn\cld\MGA\Users\[OPM-6]	CLD.mcn Domain	1/28/202511:39:00 AM			
[PII]	[PII]	CLD.mcn Domain	2/12/20257:08:50 AM			
[PII]	[PII]	APP.mcn Domain	2/12/20257:11:04 AM			
[OPM-6]	[OPM-6]@opm.gov	OD Reports : New Hire Daily Tracker Power BI - USADATA	1/31/2025			
[OPM-6]	[OPM-6]@opm.gov	OPM Data : Azure Databricks Admin + NP / PRD Azure Subscriptions [OPMData / USADATA]	1/28/2025			
[OPM-6]	[OPM-6]@opm.gov	OPM Data : Connect Platform (Az.opm.entraID.efficiencyorg.admin + Az.cio.entraID.PowerBIAdmin)	1/28/2025			
[OPM-6]	[OPM-6]@opm.gov	OPM Data : Electronic Official Personnel Folder (eOPF) - DEV/TST/QA/TRN/PRD	1/28/2025	2/6/2025		
[OPM-6]	[OPM-6]@opm.gov	OPM Data : Enterprise Human Resources Integration (EHRI) - Dev/TST/QA/PRD	1/28/2025	2/6/2025		
[OPM-6]	[OPM-6]@opm.gov	USA Staffing Core + Admin Portal - DEV/TST/STG/TRN/PRD	1/28/2025			
[OPM-6]	[OPM-6]@opm.gov	Web Admin	1/28/2025			
[OPM-18]	[OPM-18]@opm.gov	STAMP	2/3/2025			
[OPM-18]	[OPM-18]@opm.gov	USA Performance - Office of the Director	1/24/2025			
[PII]	[PII]	ITSP Cloud Intake app	1/23/2025			
[PII]	[PII]	USA Performance - Office of Communications	1/31/2025			
[OPM-6]	[OPM-6]@opm.gov	Azure DevOps	1/29/2025			
[PII]	[PII]	FOIAXpress	2/4/2025			
[OPM-6]	[OPM-6]@opm.gov	USA Performance - U.S. Office of Personnel Management	1/28/2025			
[OPM-10]	[OPM-10]@opm.gov	USA Performance - Office of the Director	2/7/2025			

Employee Name	Account Username	System Name	Date Created	Date Removed	Admin Access	Login Yes/No
[PII]	[PII]	GitHub Enterprise	1/21/2025			
[OPM-2]	\mcn\cld\MGA\Users\[OPM-2]	CLD.mcn Domain	1/28/202511:39:25 AM			
[PII]	[PII]	GitHub Enterprise	1/31/2025			
[OPM-2]	[OPM-2]@opm.gov	OPM Data : Azure Databricks Admin + NP / PRD Azure Subscriptions [OPMData / USADATA]	1/28/2025			
[PII]	[PII]	GitHub Enterprise	1/31/2025			
[OPM-2]	[OPM-2]@opm.gov	OPM Data : Connect Platform (Az.opm.entraID.efficiencyorg.admin + Az.cio.entraID.PowerBIAdmin)	1/28/2025			
[PII]	[PII]	GitHub Enterprise	1/22/2025			
[PII]	[PII]	GitHub Enterprise	1/22/2025			
[PII]	[PII]	GitHub Enterprise	1/22/2025			
[PII]	[PII]	GitHub Enterprise	1/31/2025			
[PII]	[PII]	GitHub Enterprise	1/31/2025			
[PII]	[PII]	GitHub Enterprise	1/21/2025			
[PII]	[PII]	GitHub Enterprise	1/31/2025			
[PII]	[PII]	GitHub Enterprise	1/22/2025			
[PII]	[PII]	GitHub Enterprise	1/22/2025			
[OPM-2]	[OPM-2]@opm.gov	OPM Data : Electronic Official Personnel Folder (eOPF) - DEV/TST/QA/TRN/PRD	1/28/2025	2/6/2025		
[PII]	[PII]	Carrier Connect	2/7/2025			
[PII]	[PII]	Carrier Connect	1/23/2025			
[PII]	[PII]	Carrier Connect	2/7/2025			
[PII]	[PII]	Engagement Tracking System	2/3/2025			
[PII]	[PII]	STAMP	1/23/2025			
[OPM-2]	[OPM-2]@opm.gov	OPM Data : Enterprise Human Resources Integration (EHRI) - Dev/TST/QA/PRD	1/28/2025	2/6/2025		
[PII]	[PII]	STAMP	1/23/2025			
[PII]	[PII]	STAMP	1/24/2025			
[OPM-2]	[OPM-2]@opm.gov	USA Staffing Core + Admin Portal - DEV/TST/STG/TRN/PRD	1/28/2025			
[OPM-2]	[OPM-2]@opm.gov	Web Admin	1/28/2025			
[OPM-2]	[OPM-2]@opm.gov	USA Performance - U.S. Office of Personnel Management	1/28/2025			
Scale,Amanda	adscales@opm.gov	USA Performance - U.S. Office of Personnel Management	1/20/2025			
Scales, Amanda	Amanda-Scales_opmgov	GitHub Enterprise	1/20/2025			
Scales, Amanda	Amanda.Scales@opm.gov	STAMP	1/31/2025			
[PII]	[PII]	STAMP	2/3/2025			
[PII]	[PII]	CLIA Tracking & CS Portal	1/27/2025			
[PII]	[PII]	CLIA Tracking & CS Portal	1/27/2025			
[PII]	[PII]	CLIA Tracking & CS Portal	1/28/2025			
[PII]	[PII]	CLIA Tracking & CS Portal	1/28/2025			
[PII]	[PII]	CXOne	1/24/2025			
[PII]	[PII]	Azure DevOps	1/21/2025			
[PII]	[PII]	Azure DevOps	1/21/2025			
[PII]	[PII]	Azure DevOps	1/21/2025			
[PII]	[PII]	Azure DevOps	1/21/2025			
[PII]	[PII]	Azure DevOps	1/21/2025			
[PII]	[PII]	USA Performance - Office of the Director	1/31/2025			
[PII]	[PII]	Azure DevOps	1/21/2025			
[PII]	[PII]	Azure DevOps	1/22/2025			
[PII]	[PII]	Azure DevOps	1/22/2025			
[PII]	[PII]	Azure DevOps	1/22/2025			
[PII]	[PII]	Azure DevOps	1/22/2025			
[PII]	[PII]	Azure DevOps	1/22/2025			
[PII]	[PII]	Azure DevOps	1/22/2025			
[PII]	[PII]	Azure DevOps	1/23/2025			
[PII]	[PII]	Azure DevOps	1/23/2025			
[PII]	[PII]	Azure DevOps	1/23/2025			
[PII]	[PII]	Azure DevOps	1/23/2025			
[PII]	[PII]	Azure DevOps	1/24/2025			
[PII]	[PII]	Azure DevOps	1/24/2025			
[PII]	[PII]	Azure DevOps	1/24/2025			
[PII]	[PII]	Azure DevOps	1/24/2025			
[PII]	[PII]	Azure DevOps	1/24/2025			
[OPM-13]	[OPM-13]@opm.gov	USA Performance - Office of the Director	1/31/2025			
[PII]	[PII]	Azure DevOps	1/27/2025			
[PII]	[PII]	Azure DevOps	1/27/2025			
[PII]	[PII]	Azure DevOps	1/28/2025			
[PII]	[PII]	Azure DevOps	1/28/2025			
[PII]	[PII]	Azure DevOps	1/29/2025			
[PII]	[PII]	Azure DevOps	1/29/2025			
[PII]	[PII]	STAMP	1/31/2025			
[PII]	[PII]	Azure DevOps	1/30/2025			
[PII]	[PII]	Azure DevOps	1/31/2025			
[PII]	[PII]	Azure DevOps	1/31/2025			
[PII]	[PII]	Azure DevOps	2/3/2025			
[PII]	[PII]	Azure DevOps	2/3/2025			
[PII]	[PII]	Azure DevOps	2/3/2025			
[PII]	[PII]	Azure DevOps	2/3/2025			
[PII]	[PII]	Azure DevOps	2/4/2025			
[PII]	[PII]	Azure DevOps	2/5/2025			
[PII]	[PII]	Azure DevOps	2/5/2025			
[PII]	[PII]	Azure DevOps	2/5/2025			
[PII]	[PII]	Azure DevOps	2/7/2025			
[PII]	[PII]	Azure DevOps	2/7/2025			
[PII]	[PII]	Azure DevOps	2/7/2025			
[PII]	[PII]	Azure DevOps	2/11/2025			
[PII]	[PII]	Azure DevOps	2/11/2025			
[PII]	[PII]	Azure DevOps	2/11/2025			
[PII]	[PII]	Azure DevOps	2/12/2025			
[PII]	[PII]	Azure DevOps	2/13/2025			
[PII]	[PII]	Federal Disputed Claims (FDC)	2/10/2025			
[PII]	[PII]	Federal Disputed Claims (FDC)	2/10/2025			
[PII]	[PII]	ESCS	1/20/2025			
[PII]	[PII]	USA Performance - Office of the Director	1/31/2025			
[PII]	[PII]	ESCS	2/11/2025	2/13/2025		
[PII]	[PII]	ESCS	2/14/2025			
[PII]	[PII]	ARS (ORION) - Access for this system is handled by RS	2/12/2025			
[PII]	[PII]	ARS (ORION) - Access for this system is handled by RS	2/12/2025			
[PII]	[PII]	ARS (ORION) - Access for this system is handled by RS	2/12/2025			
[PII]	[PII]	ARS (ORION) - Access for this system is handled by RS	2/12/2025			
[PII]	[PII]	ARS (ORION) - Access for this system is handled by RS	2/12/2025			
[PII]	[PII]	ARS (ORION) - Access for this system is handled by RS	2/12/2025			
[PII]	[PII]	ARS (ORION) - Access for this system is handled by RS	2/12/2025			
[PII]	[PII]	ARS (ORION) - Access for this system is handled by RS	2/12/2025			
[PII]	[PII]	ARS (ORION) - Access for this system is handled by RS	2/12/2025			
[PII]	[PII]	ARS (ORION) - Access for this system is handled by RS	2/12/2025			
[PII]	[PII]	SCRD - Access for this system is handled by RS	1/21/2025			
[PII]	[PII]	SCRD - Access for this system is handled by RS	1/22/2025			
[PII]	[PII]	SCRD - Access for this system is handled by RS	1/29/2025			
[PII]	[PII]	SCRD - Access for this system is handled by RS	1/30/2025			
[PII]	[PII]	SCRD - Access for this system is handled by RS	2/3/2025			
[PII]	[PII]	SCRD - Access for this system is handled by RS	2/6/2025			
[PII]	[PII]	SCRD - Access for this system is handled by RS	2/11/2025			
[PII]	[PII]	SCRD - Access for this system is handled by RS	1/21/2025			

Date (UTC)	Time	Service	Category	Activity	ActorDisplayName	Target1UserPrincipalName	Target1ModifiedProperty2NewValue		
1/20/2025	22:07:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Greg.Hogan@opm.gov	"opm-AllEmailGov-np-01.Contributor.RBAC"		
1/20/2025	22:07:41	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-5]@opm.gov	"opm-AllEmailGov-np-01.Contributor.RBAC"		
1/20/2025	22:07:11	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-5]@opm.gov	"opm-AllEmailGov-p-01.Contributor.RBAC"		
1/20/2025	22:07:08	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Greg.Hogan@opm.gov	"opm-AllEmailGov-p-01.Contributor.RBAC"		
1/20/2025	21:17:04	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Charles.Ezell@opm.gov	"hrs-usaj-np-001.SubContributor"		
1/20/2025	21:16:27	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Charles.Ezell@opm.gov	"hrs-usaj-p-001.Contributor"		
1/20/2025	21:15:25	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Charles.Ezell@opm.gov	"hrs-usas-prd-001.Contributor.RBAC"		
1/20/2025	21:14:04	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Charles.Ezell@opm.gov	"hrs-usas-np-001.SubContributor"		
1/20/2025	21:12:20	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Charles.Ezell@opm.gov	"hrs-usap-np-001.Contributor"		
1/20/2025	21:11:54	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Charles.Ezell@opm.gov	"hrs-usap-p-001.Contributor"		
1/20/2025	20:37:35	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Greg.Hogan@opm.gov	"hrs-usaj-p-001.Contributor"		
1/20/2025	20:37:32	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-7]@opm.gov	"hrs-usaj-p-001.Contributor"		
1/20/2025	20:37:32	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-3]@opm.gov	"hrs-usaj-p-001.Contributor"		
1/20/2025	20:37:30	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-5]@opm.gov	"hrs-usaj-p-001.Contributor"		
1/20/2025	20:37:29	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Amanda.Scales@opm.gov	"hrs-usaj-p-001.Contributor"		
1/20/2025	20:36:33	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Greg.Hogan@opm.gov	"hrs-usaj-np-001.SubContributor"		
1/20/2025	20:36:32	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-7]@opm.gov	"hrs-usaj-np-001.SubContributor"		
1/20/2025	20:36:32	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Amanda.Scales@opm.gov	"hrs-usaj-np-001.SubContributor"		
1/20/2025	20:36:29	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-3]@opm.gov	"hrs-usaj-np-001.SubContributor"		
1/20/2025	20:36:28	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-5]@opm.gov	"hrs-usaj-np-001.SubContributor"		
1/20/2025	20:35:15	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-5]@opm.gov	"hrs-usap-p-001.Contributor"		
1/20/2025	20:35:09	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-7]@opm.gov	"hrs-usap-p-001.Contributor"		
1/20/2025	20:35:02	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Greg.Hogan@opm.gov	"hrs-usap-p-001.Contributor"		
1/20/2025	20:34:59	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usap-p-001.Contributor"		
1/20/2025	20:34:57	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-3]@opm.gov	"hrs-usap-p-001.Contributor"		
1/20/2025	20:33:55	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Greg.Hogan@opm.gov	"hrs-usap-np-001.Contributor"		
1/20/2025	20:33:54	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-7]@opm.gov	"hrs-usap-np-001.Contributor"		
1/20/2025	20:33:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-3]@opm.gov	"hrs-usap-np-001.Contributor"		
1/20/2025	20:33:43	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-5]@opm.gov	"hrs-usap-np-001.Contributor"		
1/20/2025	20:33:34	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usap-np-001.Contributor"		
1/20/2025	20:31:16	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-3]@opm.gov	"hrs-usas-np-001.Contributor.RBAC"		
1/20/2025	20:30:56	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-7]@opm.gov	"hrs-usas-np-001.Contributor.RBAC"		
1/20/2025	20:30:54	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usas-np-001.Contributor.RBAC"		
1/20/2025	20:30:54	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usas-np-001.Contributor.RBAC"		
1/20/2025	20:30:52	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-5]@opm.gov	"hrs-usas-np-001.Contributor.RBAC"		
1/20/2025	20:28:15	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-3]@opm.gov	"hrs-usas-prd-001.Contributor.RBAC"		
1/20/2025	20:28:06	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-7]@opm.gov	"hrs-usas-prd-001.Contributor.RBAC"		
1/20/2025	20:27:55	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-5]@opm.gov	"hrs-usas-prd-001.Contributor.RBAC"		
1/20/2025	20:27:53	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Greg.Hogan@opm.gov	"hrs-usas-prd-001.Contributor.RBAC"		
1/20/2025	20:27:49	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usas-prd-001.Contributor.RBAC"		
1/21/2025	23:58:32	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	23:56:19	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/21/2025	23:56:04	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	20:46:33	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	20:44:55	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management		"HRS – LAB – WIC Collaboration"		
1/21/2025	20:35:29	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	19:17:53	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	19:16:57	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	18:40:05	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	18:39:39	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	18:38:55	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	18:38:53	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	18:38:08	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	18:37:57	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	18:36:36	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	18:35:46	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	18:35:34	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"ocfo-bms-p.Contributor.RBAC"		
1/21/2025	18:35:05	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"ocfo-bms-p.Owner.RBAC"		
1/21/2025	18:34:05	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"ocfo-bms-np.Contributor.RBAC"		
1/21/2025	18:32:51	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"ocfo-bms-np.Owner.RBAC"		
1/21/2025	18:15:45	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Greg.Hogan@opm.gov	"CIITAR Application Users"		
1/21/2025	17:41:09	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"CIITAR Application Users"		
1/21/2025	17:41:03	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"CIITAR Application Users"		
1/21/2025	16:27:00	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	16:22:32	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"rg-hrs-opf-dev-document-intelligence.RBAC"		
1/21/2025	15:19:14	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	15:19:14	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	14:44:52	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	14:40:03	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	14:34:32	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"GHEC-OPM-OCIO-FITBS-HRSITPMO-USAData-Members"		
1/21/2025	14:34:32	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"OPM-GHEC-User-Read"		
1/21/2025	14:32:43	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"GHEC-OPM-OCIO-FITBS-HRSITPMO-USAData-Members"		
1/21/2025	14:32:43	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"OPM-GHEC-User-Read"		
1/21/2025	14:19:51	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	14:16:10	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	13:59:11	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"eid-eopf-helpdesk-footprints-apppxy-users"		
1/21/2025	13:58:51	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"eid-eopf-helpdesk-footprints-apppxy-users"		
1/21/2025	13:38:52	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	13:35:53	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	13:18:59	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	13:18:41	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	8:59:47	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	8:59:29	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	8:59:27	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	8:59:08	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	8:58:35	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	8:57:43	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	8:57:18	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	8:57:11	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	8:57:10	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	8:57:04	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-3]@opm.gov	"Az.OPM.LearningConnection.Prod.User"		
1/21/2025	8:56:55	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	8:56:54	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	8:56:53	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	8:56:15	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	8:55:31	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-3]@opm.gov	"AZ.OPM.KnowBe4.User"		
1/21/2025	8:55:26	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/21/2025	3:20:38	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-3]@opm.gov	"opm-AllEmailGov-p-01.Contributor.RBAC"		
1/21/2025	3:20:28	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-3]@opm.gov	"opm-AllEmailGov-p-01.Contributor.RBAC"		
1/21/2025	3:02:58	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-3]@opm.gov	"opm-AllEmailGov-p-01.Contributor.RBAC"		
1/21/2025	3:02:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-3]@opm.gov	"opm-AllEmailGov-np-01.Contributor.RBAC"		
1/21/2025	3:01:43	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-3]@opm.gov	"opm-AllEmailGov-np-01.Contributor.RBAC"		
1/21/2025	2:35:59	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-3]@opm.gov	"opm-AllEmailGov-np-01.Contributor.RBAC"		
1/21/2025	2:35:23	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-3]@opm.gov	"opm-AllEmailGov-p-01.Contributor.RBAC"		
1/21/2025	0:14:34	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Greg.Hogan@opm.gov	"AZ.Serv-Support-Admin"		
1/22/2025	22:45:43	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-7]@opm.gov	"OPM-GHEC-User-Read"		
1/22/2025	22:45:43	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-7]@opm.gov	"GHEC-OPM-OD-Owners"		
1/22/2025	22:45:41	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Amanda.Scales@opm.gov	"OPM-GHEC-User-Read"		
1/22/2025	22:45:41	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-5]@opm.gov	"OPM-GHEC-User-Read"		
1/22/2025	22:45:40	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-5]@opm.gov	"GHEC-OPM-OD-Owners"		
1/22/2025	22:45:40	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-3]@opm.gov	"OPM-GHEC-User-Read"		
1/22/2025	22:45:40	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Amanda.Scales@opm.gov	"GHEC-OPM-OD-Owners"		
1/22/2025	22:45:39	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-3]@opm.gov	"GHEC-OPM-OD-Owners"		
1/22/2025	22:45:37	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Greg.Hogan@opm.gov	"OPM-GHEC-User-Read"		
1/22/2025	22:45:36	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Greg.Hogan@opm.gov	"GHEC-OPM-OD-Owners"		
1/22/2025	22:45:36	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Charles.Ezell@opm.gov	"GHEC-OPM-OD-Owners"		
1/22/2025	22:00:25	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"ghec.emu.Enterprise.Owners"		
1/22/2025	21:59:41	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/22/2025	21:52:24	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"ghec.emu.Enterprise.Owners"		
1/22/2025	21:52:23	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-3]@opm.gov	"ghec.emu.Enterprise.Owners"		
1/22/2025	21:52:22	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-7]@opm.gov	"ghec.emu.Enterprise.Owners"		
1/22/2025	21:52:22	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"ghec.emu.Enterprise.Owners"		

Date (UTC)	Time	Service	Category	Activity	ActorDisplayName	Target1UserPrincipalName	Target1ModifiedProperty2NewValue		
1/22/2025	21:52:21	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"ghec.emu.Enterprise.Owners"		
1/22/2025	21:52:21	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"ghec.emu.Enterprise.Owners"		
1/22/2025	21:52:20	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Greg.Hogan@opm.gov	"ghec.emu.Enterprise.Owners"		
1/22/2025	21:52:19	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-5]@opm.gov	"ghec.emu.Enterprise.Owners"		
1/22/2025	21:52:17	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"ghec.emu.Enterprise.Owners"		
1/22/2025	21:52:17	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"ghec.emu.Enterprise.Owners"		
1/22/2025	21:52:14	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"ghec.emu.Enterprise.Owners"		
1/22/2025	21:52:12	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"ghec.emu.Enterprise.Owners"		
1/22/2025	21:52:11	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"ghec.emu.Enterprise.Owners"		
1/22/2025	21:52:10	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Amanda.Scales@opm.gov	"ghec.emu.Enterprise.Owners"		
1/22/2025	21:52:08	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"ghec.emu.Enterprise.Owners"		
1/22/2025	19:29:52	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.CHCODocRepo.Prod.User"		
1/22/2025	19:29:22	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-3]@opm.gov	"Az.OPM.CHCODocRepo.Prod.User"		
1/22/2025	19:16:58	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"az.hcdmm.rio.web.dev.readonly"		
1/22/2025	18:58:12	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"OCIO-STAMP-Users"		
1/22/2025	18:36:53	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Charles.Ezell@opm.gov	"OCIO-STAMP-Users"		
1/22/2025	17:03:35	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.Security-SOCIr-Resources-Team"		
1/22/2025	17:02:47	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/22/2025	17:02:47	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/22/2025	17:02:46	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/22/2025	17:02:45	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/22/2025	17:02:45	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/22/2025	17:02:44	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/22/2025	17:02:43	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/22/2025	17:02:42	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/22/2025	15:55:58	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.Purview-IRM-Investigators"		
1/22/2025	15:55:57	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.rg-cyber-playbooks-p-001.Contributor"		
1/22/2025	15:54:09	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/22/2025	15:53:43	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.Purview-IRM-Investigators"		
1/22/2025	15:53:42	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.Security.Admin"		
1/22/2025	15:53:41	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.rg-cyber-playbooks-p-001.Contributor"		
1/22/2025	15:53:41	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"ocio-cyber-p-001.Contributor.RBAC"		
1/22/2025	15:49:57	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"ocio-cyber-p-001.Reader.RBAC"		
1/22/2025	15:49:56	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"rg-AzLogs-p-001.Contributor.RBAC"		
1/22/2025	15:49:56	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.Sentinel.LogApp.Contributor"		
1/22/2025	15:49:55	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"rg-AzLogs-p-001.Reader"		
1/22/2025	15:49:55	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"OCIO – Cloud Services"		
1/22/2025	15:49:54	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.Compliance-Data-Admin"		
1/22/2025	15:49:54	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.Security-DataProtection-Team"		
1/22/2025	15:49:53	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.Compliance.Admin"		
1/22/2025	15:49:53	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.AAD.GlobalReader"		
1/22/2025	15:49:52	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.Global.Reader.RBAC"		
1/22/2025	15:49:52	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.Security.Reader"		
1/22/2025	15:44:37	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"WIZ-USAP-Reader"		
1/22/2025	15:40:25	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"WIZ-USAP-Reader"		
1/22/2025	15:40:24	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"WIZ-USAP-Reader"		
1/22/2025	15:36:47	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"GHEC-OPM-HI-Members"		
1/22/2025	15:36:46	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"OPM-GHEC-User-Read"		
1/22/2025	15:34:00	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"OPM-GHEC-User-Read"		
1/22/2025	15:33:59	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"GHEC-OPM-OCIO-BAS-OPM-APS-PP-Members"		
1/22/2025	15:32:53	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"GHEC-OPM-OCIO-FITBS-HRSITPMO-USALearning-Members"		
1/22/2025	15:32:49	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"OPM-GHEC-User-Read"		
1/22/2025	15:32:48	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"GHEC-OPM-OCIO-BAS-OPM-APS-PP-Members"		
1/22/2025	15:32:03	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"OPM-GHEC-User-Read"		
1/22/2025	15:32:03	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"GHEC-OPM-OCIO-BAS-OPM-APS-PP-Members"		
1/22/2025	15:30:58	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"OPM-GHEC-User-Read"		
1/22/2025	15:30:57	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"GHEC-OPM-OCIO-BAS-OPM-APS-PP-Members"		
1/22/2025	15:10:20	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"OCIO-STAMP-Users"		
1/22/2025	14:53:20	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"iRetireStage"		
1/22/2025	14:51:00	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"iRetireProd"		
1/22/2025	14:26:37	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"eid-usas-footprints-apppxy-users"		
1/22/2025	14:26:26	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"eid-usas-footprints-apppxy-users"		
1/22/2025	14:26:14	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"eid-usas-footprints-apppxy-users"		
1/22/2025	5:07:12	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/22/2025	5:07:11	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/22/2025	1:46:25	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/22/2025	1:37:55	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/22/2025	1:09:35	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/22/2025	1:09:19	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/22/2025	1:08:10	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/22/2025	1:05:59	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/22/2025	0:49:37	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/22/2025	0:47:44	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/22/2025	0:47:43	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/22/2025	0:47:36	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/22/2025	0:47:18	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/22/2025	0:45:46	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/22/2025	0:18:44	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/22/2025	0:18:34	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/22/2025	0:18:22	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/23/2025	22:10:51	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	21:55:33	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	20:02:48	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"GHEC-OPM-OCIO-FITBS-HRSITPMO-USAS-Architects"		
1/23/2025	19:56:08	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/23/2025	19:55:32	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/23/2025	19:48:42	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/23/2025	19:36:13	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/23/2025	19:29:44	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	19:18:12	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Invicti.User"		
1/23/2025	19:18:04	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Invicti.User"		
1/23/2025	19:12:32	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	19:11:42	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	19:11:42	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	19:11:41	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	19:11:40	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	19:11:39	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	19:11:39	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	19:11:38	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	19:11:37	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	19:11:37	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	19:10:40	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	19:10:39	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	19:10:38	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	19:10:38	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	18:48:37	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-4]@opm.gov	"AZ.OPM.KnowBe4.User"		
1/23/2025	18:47:00	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov	"AZ.OPM.KnowBe4.User"		
1/23/2025	18:44:34	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov	"Az.OPM.LearningConnection.Prod.User"		
1/23/2025	18:42:38	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-4]@opm.gov	"Az.OPM.LearningConnection.Prod.User"		
1/23/2025	18:23:17	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	18:23:04	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"cto-digitalservices-np-01.Contributor.RBAC"		
1/23/2025	17:56:33	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	ADScales@opm.gov	"AZ.OPM.KnowBe4.User"		
1/23/2025	17:55:32	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	ADScales@opm.gov	"Az.OPM.LearningConnection.Prod.User"		
1/23/2025	17:44:09	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	17:43:55	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"cto-digitalservices-np-01.Owner.RBAC"		
1/23/2025	17:00:02	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/23/2025	16:59:11	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/23/2025	16:56:37	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/23/2025	16:56:15	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/23/2025	16:56:15	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/23/2025	16:55:22	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/23/2025	16:46:20	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	16:46:03	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			

Date (UTC)	Time	Service	Category	Activity	ActorDisplayName	Target1UserPrincipalName	Target1ModifiedProperty2NewValue		
1/23/2025	16:38:59	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"cto-digitalservices-np-01.Contributor.RBAC"		
1/23/2025	16:02:49	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"cto-digitalservices-np-01.Contributor.RBAC"		
1/23/2025	16:02:22	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	16:02:21	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	16:02:20	Core Directory	UserManagement	Update user	Azure AD Identity Governance - Directory Management	[PII]	"AccountEnabled"		
1/23/2025	16:02:20	Core Directory	UserManagement	Disable account	Azure AD Identity Governance - Directory Management	[PII]	"AccountEnabled"		
1/23/2025	15:59:01	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	15:58:55	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"OCIO-STAMP-Users"		
1/23/2025	15:12:46	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.Security-Operators"		
1/23/2025	15:12:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.Security-Operators"		
1/23/2025	15:10:09	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	15:09:37	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	14:57:22	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	14:56:59	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	14:56:35	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	14:55:59	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	14:55:35	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	14:55:08	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	14:53:14	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	14:52:38	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	14:51:56	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	14:49:31	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	14:47:43	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	14:45:45	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	14:44:33	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	13:49:21	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	13:34:01	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-opmdata-p-001.Reader"		
1/23/2025	13:30:21	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	13:22:58	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"az.databrx.data.analyst.ehri"		
1/23/2025	13:21:41	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	13:21:23	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"az.databrx.data.engineer.hbdp.postal.prd"		
1/23/2025	13:21:23	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"az.databrx.data.engineer.hbdp.postal.prd"		
1/23/2025	13:19:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"az.databrx.data.analyst.usadata.dev"		
1/23/2025	13:17:06	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"az.databrx.data.analyst.usadata.prod"		
1/23/2025	13:16:39	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"az.databrx.data.analyst.usadata.dev"		
1/23/2025	9:24:00	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/23/2025	9:23:17	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/23/2025	9:22:29	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/23/2025	9:20:13	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/23/2025	9:18:39	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/23/2025	9:18:30	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/23/2025	9:18:01	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/23/2025	9:17:28	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/23/2025	9:17:14	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/23/2025	9:16:50	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/23/2025	9:16:26	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/23/2025	9:16:05	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/23/2025	9:16:02	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/23/2025	9:15:38	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/23/2025	9:15:30	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/23/2025	9:15:26	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/24/2025	22:08:20	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"cto-digitalservices-np-01.Contributor.RBAC"		
1/24/2025	21:52:43	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/24/2025	21:34:56	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Box.SFT.AppUsers"		
1/24/2025	21:22:12	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"cto-digitalservices-np-01.Owner.RBAC"		
1/24/2025	21:10:19	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/24/2025	21:10:17	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/24/2025	20:58:11	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"OCIO-STAMP-Users"		
1/24/2025	20:58:09	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"OCIO-STAMP-Users"		
1/24/2025	18:31:54	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-opf-p-001.Contributor.RBAC"		
1/24/2025	18:30:10	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usap-np-001.Reader"		
1/24/2025	15:51:31	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usap-p-001.Reader"		
1/24/2025	15:15:06	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"OCIO-STAMP-Users"		
1/24/2025	15:09:51	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"ocio-hcdmm-ai-np.Contributor.RBAC"		
1/24/2025	15:09:22	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.CogServices-AI-Contributor-HCDMM"		
1/24/2025	11:57:08	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.USAStaffingLMSUdutu.Prod.User"		
1/25/2025	17:48:09	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/25/2025	17:28:07	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/25/2025	9:30:36	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/25/2025	9:30:19	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/25/2025	9:30:00	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/25/2025	9:29:48	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/25/2025	9:29:35	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/25/2025	9:29:31	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/25/2025	9:29:27	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/25/2025	9:28:24	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/25/2025	9:28:08	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/25/2025	9:27:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/25/2025	9:27:18	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/25/2025	9:27:18	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/25/2025	9:27:12	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/25/2025	9:27:02	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-16]@opm.gov	"AZ.OPM.KnowBe4.User"		
1/25/2025	9:26:26	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-16]@opm.gov	"Az.OPM.LearningConnection.Prod.User"		
1/25/2025	9:25:40	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/25/2025	9:25:25	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/25/2025	9:25:21	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/27/2025	22:09:51	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/27/2025	22:09:28	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/27/2025	22:08:21	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/27/2025	22:06:59	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/27/2025	22:06:20	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/27/2025	22:05:59	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/27/2025	21:06:27	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/27/2025	21:05:27	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/27/2025	20:34:09	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/27/2025	20:30:24	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/27/2025	20:28:21	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/27/2025	20:25:33	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/27/2025	20:25:30	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"eid-bsgportal-apppxy-users"		
1/27/2025	19:21:14	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Apptio.Cloudability.Admin"		
1/27/2025	18:40:14	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/27/2025	18:28:57	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/27/2025	18:24:26	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"OCIO-STAMP-Users"		
1/27/2025	18:24:14	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/27/2025	18:14:42	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/27/2025	18:09:52	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/27/2025	18:07:31	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/27/2025	18:05:36	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/27/2025	17:29:47	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"ocio-hcdmm-ai-np.DocumentIntelligence"		
1/27/2025	17:27:04	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/27/2025	17:26:53	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/27/2025	17:09:39	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.USAStaffingLMS.Prod.User"		
1/27/2025	16:17:47	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.USAPerformanceLMS.Prod.User"		
1/27/2025	16:17:46	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.USAPerformanceLMS.Prod.User"		
1/27/2025	15:53:41	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/27/2025	15:52:32	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"az.hcdmm.rio.web.dev.businesssteward"		
1/27/2025	15:50:48	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/27/2025	14:32:03	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/27/2025	14:27:46	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"eid-bsgportal-apppxy-users"		
1/27/2025	14:27:20	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/27/2025	4:09:02	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/28/2025	22:34:41	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Greg.Hogan@opm365.onmicrosoft.com	"AZ.Global-Admin"		

Date (UTC)	Time	Service	Category	Activity	ActorDisplayName	Target1UserPrincipalName	Target1ModifiedProperty2NewValue		
1/28/2025	21:57:26	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	Greg.Hogan@opm365.onmicrosoft.com			
1/28/2025	21:21:00	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-2]@opm.gov	"hrs-opf-np-001.Contributor.RBAC"		
1/28/2025	21:20:59	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov	"hrs-opf-np-001.Contributor.RBAC"		
1/28/2025	21:20:59	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-4]@opm.gov	"hrs-opf-np-001.Contributor.RBAC"		
1/28/2025	21:20:19	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-2]@opm.gov	"hrs-opf-p-001.Contributor.RBAC"		
1/28/2025	21:20:07	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-4]@opm.gov	"hrs-opf-p-001.Contributor.RBAC"		
1/28/2025	21:20:00	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov	"hrs-opf-p-001.Contributor.RBAC"		
1/28/2025	21:14:28	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/28/2025	21:14:27	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/28/2025	21:14:27	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/28/2025	21:10:18	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-3]@opm.gov	"GitHub-Global-Owner"		
1/28/2025	21:10:13	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Amanda.Scales@opm.gov	"GitHub-Global-Owner"		
1/28/2025	21:10:13	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-5]@opm.gov	"GitHub-Global-Owner"		
1/28/2025	21:10:13	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Greg.Hogan@opm.gov	"GitHub-Global-Owner"		
1/28/2025	21:10:12	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-7]@opm.gov	"GitHub-Global-Owner"		
1/28/2025	21:05:38	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-2]@opm.gov	"GitHub-Global-Owner"		
1/28/2025	21:05:37	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-2]@opm.gov	"OPM-GHEC-User-Read"		
1/28/2025	21:05:36	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov	"GitHub-Global-Owner"		
1/28/2025	21:05:36	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov	"OPM-GHEC-User-Read"		
1/28/2025	21:05:33	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-4]@opm.gov	"GitHub-Global-Owner"		
1/28/2025	21:05:33	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-4]@opm.gov	"OPM-GHEC-User-Read"		
1/28/2025	20:53:13	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Greg.Hogan@opm365.onmicrosoft.com	"AZ.Global-Admin"		
1/28/2025	19:58:51	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.CLDCentral.Prod.User"		
1/28/2025	19:48:19	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-4]@opm.gov	"hrs-opmdata-qa-001.SubContributor.RBAC"		
1/28/2025	19:48:11	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-2]@opm.gov	"hrs-opmdata-qa-001.SubContributor.RBAC"		
1/28/2025	19:48:08	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov	"hrs-opmdata-qa-001.SubContributor.RBAC"		
1/28/2025	19:47:35	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-2]@opm.gov	"hrs-opmdata-p-001.SubContributor"		
1/28/2025	19:47:32	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov	"hrs-opmdata-p-001.SubContributor"		
1/28/2025	19:47:32	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-4]@opm.gov	"hrs-opmdata-p-001.SubContributor"		
1/28/2025	19:45:54	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-4]@opm.gov	"hrs-opmdata-001.Contributor"		
1/28/2025	19:45:54	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-2]@opm.gov	"hrs-opmdata-001.Contributor"		
1/28/2025	19:45:52	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov	"hrs-opmdata-001.Contributor"		
1/28/2025	19:40:27	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov	"hrs-usad-p-001.Contributor.RBAC"		
1/28/2025	19:40:16	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-2]@opm.gov	"hrs-usad-p-001.Contributor.RBAC"		
1/28/2025	19:40:15	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-4]@opm.gov	"hrs-usad-p-001.Contributor.RBAC"		
1/28/2025	19:39:26	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-2]@opm.gov	"hrs-usad-qa-001.Contributor.RBAC"		
1/28/2025	19:39:20	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov	"hrs-usad-qa-001.Contributor.RBAC"		
1/28/2025	19:39:19	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-4]@opm.gov	"hrs-usad-qa-001.Contributor.RBAC"		
1/28/2025	19:38:34	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-2]@opm.gov	"hrs-usad-dev-001.Contributor.RBAC"		
1/28/2025	19:38:34	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-4]@opm.gov	"hrs-usad-dev-001.Contributor.RBAC"		
1/28/2025	19:38:33	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov	"hrs-usad-dev-001.Contributor.RBAC"		
1/28/2025	19:20:46	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Greg.Hogan@opm365.onmicrosoft.com	"AZ.Exchange-Admin"		
1/28/2025	18:51:09	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.Global-Admin"		
1/28/2025	18:27:24	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/28/2025	18:27:23	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/28/2025	18:27:22	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/28/2025	18:15:58	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/28/2025	18:15:50	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/28/2025	18:15:44	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/28/2025	18:15:42	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/28/2025	16:22:51	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/28/2025	16:22:47	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/28/2025	16:22:46	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/28/2025	16:22:44	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/28/2025	16:17:16	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"ghec.emu.Enterprise.Owners"		
1/28/2025	16:17:16	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov	"ghec.emu.Enterprise.Owners"		
1/28/2025	16:17:16	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"ghec.emu.Enterprise.Owners"		
1/28/2025	16:17:16	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-2]@opm.gov	"ghec.emu.Enterprise.Owners"		
1/28/2025	16:17:15	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"ghec.emu.Enterprise.Owners"		
1/28/2025	16:17:14	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"ghec.emu.Enterprise.Owners"		
1/28/2025	16:17:11	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-4]@opm.gov	"ghec.emu.Enterprise.Owners"		
1/28/2025	16:16:15	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"OPM Amazon Business - CIO"		
1/28/2025	16:13:47	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"OPM Amazon Business - OCFO"		
1/28/2025	15:58:05	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/28/2025	15:44:43	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-4]@opm.gov	"hrs-usaj-p-001.Contributor"		
1/28/2025	15:44:41	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov	"hrs-usaj-p-001.Contributor"		
1/28/2025	15:44:39	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-2]@opm.gov	"hrs-usaj-p-001.Contributor"		
1/28/2025	15:44:04	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.CyberAdmin.UAT"		
1/28/2025	15:43:48	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-4]@opm.gov	"hrs-usaj-np-001.SubContributor"		
1/28/2025	15:43:46	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-2]@opm.gov	"hrs-usaj-np-001.SubContributor"		
1/28/2025	15:43:46	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov	"hrs-usaj-np-001.SubContributor"		
1/28/2025	15:43:15	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.CyberAdmin.DEV"		
1/28/2025	15:42:53	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.CyberAdmin.PERF"		
1/28/2025	15:42:48	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-2]@opm.gov	"hrs-usap-p-001.Contributor"		
1/28/2025	15:42:42	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.CyberAdmin.SIT"		
1/28/2025	15:42:16	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov	"hrs-usap-p-001.Contributor"		
1/28/2025	15:42:11	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-4]@opm.gov	"hrs-usap-p-001.Contributor"		
1/28/2025	15:41:11	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov	"hrs-usap-np-001.Contributor"		
1/28/2025	15:41:10	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-4]@opm.gov	"hrs-usap-np-001.Contributor"		
1/28/2025	15:41:07	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-2]@opm.gov	"hrs-usap-np-001.Contributor"		
1/28/2025	15:40:10	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-2]@opm.gov	"hrs-usas-prd-001.Contributor.RBAC"		
1/28/2025	15:40:06	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-4]@opm.gov	"hrs-usas-prd-001.Contributor.RBAC"		
1/28/2025	15:40:06	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov	"hrs-usas-prd-001.Contributor.RBAC"		
1/28/2025	15:39:33	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov	"hrs-usas-np-001.SubContributor"		
1/28/2025	15:39:32	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-4]@opm.gov	"hrs-usas-np-001.SubContributor"		
1/28/2025	15:38:57	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-2]@opm.gov	"hrs-usas-np-001.SubContributor"		
1/28/2025	15:29:30	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-retsys-np-001.Key.Vault.Contributor.RBAC"		
1/28/2025	15:29:30	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-retsys-np-001.Key.Vault.Contributor.RBAC"		
1/28/2025	15:29:28	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-retsys-np-001.Key.Vault.Contributor.RBAC"		
1/28/2025	15:29:28	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-retsys-np-001.Key.Vault.Contributor.RBAC"		
1/28/2025	15:29:28	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-retsys-np-001.Key.Vault.Contributor.RBAC"		
1/28/2025	15:29:27	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-retsys-np-001.Key.Vault.Contributor.RBAC"		
1/28/2025	15:29:26	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-retsys-np-001.Key.Vault.Contributor.RBAC"		
1/28/2025	15:29:26	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-retsys-np-001.Key.Vault.Contributor.RBAC"		
1/28/2025	15:29:25	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-retsys-np-001.Key.Vault.Contributor.RBAC"		
1/28/2025	15:29:25	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-retsys-np-001.Key.Vault.Contributor.RBAC"		
1/28/2025	15:29:25	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-retsys-np-001.Key.Vault.Contributor.RBAC"		
1/28/2025	15:29:24	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-retsys-np-001.Key.Vault.Contributor.RBAC"		
1/28/2025	13:04:04	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usal-np-001.Contributor.RBAC"		
1/28/2025	13:03:23	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usal-np-001.Contributor.RBAC"		
1/28/2025	13:03:22	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usal-np-001.Contributor.RBAC"		
1/28/2025	13:03:22	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usal-np-001.Contributor.RBAC"		
1/28/2025	13:03:19	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usal-np-001.Contributor.RBAC"		
1/28/2025	13:03:15	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usal-np-001.Contributor.RBAC"		
1/28/2025	13:03:13	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usal-np-001.Contributor.RBAC"		
1/28/2025	13:03:12	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usal-np-001.Contributor.RBAC"		
1/28/2025	13:03:11	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usal-np-001.Contributor.RBAC"		
1/28/2025	13:03:11	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usal-np-001.Contributor.RBAC"		
1/28/2025	12:08:03	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Box.SFT.AppUsers"		
1/28/2025	5:05:59	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/28/2025	5:05:58	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/28/2025	5:05:57	Core Directory	UserManagement	Disable account	Azure AD Identity Governance - Directory Management	[PII]	"AccountEnabled"		
1/28/2025	5:05:57	Core Directory	UserManagement	Update user	Azure AD Identity Governance - Directory Management	[PII]	"AccountEnabled"		
1/28/2025	5:02:35	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-opf-p-001.StorageBlobDataContributor.RBAC"		
1/28/2025	0:30:54	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-5]@opm.gov	"AZ.Global.Reader.RBAC"		
1/28/2025	0:30:54	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Greg.Hogan@opm.gov	"AZ.Global.Reader.RBAC"		
1/28/2025	0:30:18	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-5]@opm.gov	"AZ.AAD.GlobalReader"		
1/28/2025	0:30:15	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Greg.Hogan@opm.gov	"AZ.AAD.GlobalReader"		
1/29/2025	23:03:33	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov	"AZ.AAD.GlobalReader"		
1/29/2025	22:35:01	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:34:50	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:34:47	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		

Date (UTC)	Time	Service	Category	Activity	ActorDisplayName	Target1UserPrincipalName	Target1ModifiedProperty2NewValue		
1/29/2025	22:34:45	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:34:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:34:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:33:55	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:33:53	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:33:45	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:33:45	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:33:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:32:57	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:32:56	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:32:56	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:32:56	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:32:55	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:32:52	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:32:52	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:32:48	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:32:48	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:32:48	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:32:48	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:32:47	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:32:47	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:32:47	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:32:47	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:32:47	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:32:47	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:32:47	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:32:47	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:32:47	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:32:46	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:32:46	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:32:46	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:32:46	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:32:46	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:32:45	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	22:32:45	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.SIT"		
1/29/2025	21:57:46	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:46	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:46	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:45	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:45	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:45	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:45	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:45	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:45	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:45	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:45	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:43	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:43	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:43	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:43	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:43	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:43	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:43	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:42	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:42	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:42	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:42	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:42	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:42	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:42	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:41	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:41	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:41	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:41	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:41	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:41	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:41	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:41	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:41	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:40	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:40	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:39	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:39	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:39	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:39	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:38	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:38	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:57:38	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.UAT"		
1/29/2025	21:44:56	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.USAStaffingLMS.Prod.User"		
1/29/2025	21:36:57	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"OCIO-STAMP-Users"		
1/29/2025	21:36:06	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"OCIO-STAMP-Users"		
1/29/2025	20:31:17	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.USAS-dev-dataplane-resources-Team"		
1/29/2025	20:30:35	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.USAS-dev-controlplane-resources-Team"		
1/29/2025	19:51:19	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Alfabet.Prod"		
1/29/2025	19:51:18	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Alfabet.Prod"		
1/29/2025	19:49:04	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Alfabet.Test"		
1/29/2025	19:49:03	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Alfabet.Test"		
1/29/2025	19:48:26	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Dockerhub.User"		
1/29/2025	19:48:25	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Dockerhub.User"		
1/29/2025	19:48:25	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Dockerhub.User"		
1/29/2025	19:48:25	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Dockerhub.User"		
1/29/2025	19:48:23	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Dockerhub.User"		
1/29/2025	19:48:23	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Dockerhub.User"		
1/29/2025	19:48:23	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Dockerhub.User"		
1/29/2025	19:48:23	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Dockerhub.User"		
1/29/2025	19:48:22	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Dockerhub.User"		
1/29/2025	19:48:19	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Dockerhub.User"		
1/29/2025	19:40:50	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Alfabet.Dev"		
1/29/2025	19:40:50	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Alfabet.Dev"		
1/29/2025	19:18:57	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[OPM-2]@opm.gov			

Date (UTC)	Time	Service	Category	Activity	ActorDisplayName	Target1UserPrincipalName	Target1ModifiedProperty2NewValue		
1/29/2025	19:18:41	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov			
1/29/2025	19:18:37	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[OPM-5]@opm.gov			
1/29/2025	19:18:23	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	Amanda.Scales@opm.gov			
1/29/2025	19:18:21	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[OPM-7]@opm.gov			
1/29/2025	19:18:13	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[OPM-3]@opm.gov			
1/29/2025	19:18:09	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[OPM-4]@opm.gov			
1/29/2025	17:43:05	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	Greg.Hogan@opm.gov			
1/29/2025	17:30:52	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management		"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:30:51	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management		"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:30:51	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management		"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:30:49	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management		"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:30:49	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management		"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:30:49	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management		"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:30:49	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management		"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:30:48	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management		"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:30:47	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management		"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:30:47	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management		"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:30:47	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management		"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:30:45	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management		"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:30:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management		"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:30:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management		"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:30:43	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management		"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:30:43	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management		"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:10:19	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management		"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:10:17	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management		"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:10:16	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management		"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:10:16	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management		"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:01:42	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:01:42	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:01:42	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:01:42	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:01:42	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:01:40	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:01:39	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:01:38	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:01:38	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:01:37	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:01:37	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	17:01:37	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-retsys-np-001.Key.Vault.Secrets.User.RBAC"		
1/29/2025	15:02:33	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.Prod"		
1/29/2025	15:02:32	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.Prod"		
1/29/2025	15:02:23	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.Prod"		
1/29/2025	14:37:39	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-opmhi-np-001.Contributor.RBAC"		
1/29/2025	14:37:36	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-opmhi-np-001.Contributor.RBAC"		
1/29/2025	14:36:08	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-opmhi-np-001.Reader.RBAC"		
1/29/2025	14:36:00	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-opmhi-np-001.Reader.RBAC"		
1/29/2025	14:22:01	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"eid-cliaconnect-apppxy-users"		
1/29/2025	14:20:22	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"eid-bsgportal-apppxy-users"		
1/29/2025	14:20:20	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"eid-bsgportal-apppxy-users"		
1/29/2025	14:20:13	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"eid-bsgportal-apppxy-users"		
1/29/2025	14:20:11	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"eid-bsgportal-apppxy-users"		
1/29/2025	9:50:05	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/29/2025	9:50:05	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/29/2025	9:49:52	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/29/2025	9:49:43	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-13]@opm.gov	"AZ.OPM.KnowBe4.User"		
1/29/2025	9:49:42	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/29/2025	9:49:18	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/29/2025	9:49:16	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/29/2025	9:48:12	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/29/2025	9:48:04	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/29/2025	9:48:04	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-13]@opm.gov	"Az.OPM.LearningConnection.Prod.User"		
1/29/2025	9:48:00	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/29/2025	9:47:33	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-17]@opm.gov	"AZ.OPM.KnowBe4.User"		
1/29/2025	9:47:09	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/29/2025	9:46:57	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/29/2025	9:46:22	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-17]@opm.gov	"Az.OPM.LearningConnection.Prod.User"		
1/29/2025	9:46:17	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/29/2025	9:46:05	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/29/2025	9:45:29	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/29/2025	2:07:40	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-2]@opm.gov	"opm-AllEmailGov-np-01.Contributor.RBAC"		
1/29/2025	2:07:09	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-2]@opm.gov	"opm-AllEmailGov-p-01.Contributor.RBAC"		
1/30/2025	22:05:19	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Box.SFT.AppUsers"		
1/30/2025	19:14:29	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/30/2025	19:13:28	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/30/2025	17:47:00	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"CIITAR Application Users"		
1/30/2025	17:07:20	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Apptio.Cloudability.User"		
1/30/2025	17:02:34	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/30/2025	16:50:22	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.CogServices-AI-Contributor-HCDMM"		
1/30/2025	16:50:06	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Apptio.Cloudability.User"		
1/30/2025	16:49:01	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"ocio-hcdmm-ai-np.DocumentIntelligence"		
1/30/2025	16:18:29	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov	"opm-AllEmailGov-np-01.Contributor.RBAC"		
1/30/2025	16:17:52	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov	"opm-AllEmailGov-p-01.Contributor.RBAC"		
1/30/2025	14:49:27	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Apptio.Cloudability.User"		
1/30/2025	14:48:07	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/30/2025	14:43:50	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PERF"		
1/30/2025	14:43:47	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PERF"		
1/30/2025	14:43:45	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PERF"		
1/30/2025	14:43:45	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PERF"		
1/30/2025	14:43:43	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PERF"		
1/30/2025	14:42:19	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:18	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:18	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:18	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:18	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:17	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:17	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:17	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:17	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:17	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:17	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:16	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:16	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:16	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:16	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:16	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:16	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:16	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:16	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:16	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:15	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:15	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:15	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:15	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:15	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:15	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:15	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:14	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:14	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:14	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:14	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:14	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:13	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		

Date (UTC)	Time	Service	Category	Activity	ActorDisplayName	Target1UserPrincipalName	Target1ModifiedProperty2NewValue		
1/30/2025	14:42:13	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:13	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:13	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:13	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:13	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:12	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:12	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:12	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:12	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:12	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:12	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:12	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:12	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:11	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:11	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:11	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:11	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:11	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:11	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:11	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:10	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:10	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:10	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:10	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:10	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:09	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:09	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:09	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:09	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:08	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:08	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:08	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:08	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:08	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:08	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:42:07	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.PREPROD"		
1/30/2025	14:29:39	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Apptio.Cloudability.User"		
1/30/2025	14:24:47	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.Admin"		
1/30/2025	14:24:41	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.Admin"		
1/30/2025	14:24:34	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.Admin"		
1/30/2025	14:20:43	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.Dev"		
1/30/2025	14:20:43	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.Dev"		
1/30/2025	14:20:43	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.Dev"		
1/30/2025	14:20:43	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.Dev"		
1/30/2025	14:20:42	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.Dev"		
1/30/2025	14:20:42	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.Dev"		
1/30/2025	14:20:41	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.Dev"		
1/30/2025	14:20:41	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.Dev"		
1/30/2025	14:20:41	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.Dev"		
1/30/2025	14:20:41	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.Dev"		
1/30/2025	14:18:46	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.PSHB.OPMAdmin.Dev"		
1/30/2025	1:05:33	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-4]@opm.gov	"hrs-mgmt-p-001.USAS.AppInsights.Reader"		
1/30/2025	1:05:24	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-2]@opm.gov	"hrs-mgmt-p-001.USAS.AppInsights.Reader"		
1/30/2025	1:04:29	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov	"hrs-mgmt-p-001.USAS.AppInsights.Reader"		
1/30/2025	0:31:12	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov	"AZ.Global.Reader.RBAC"		
1/31/2025	22:59:52	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Box.SFT.AppUsers"		
1/31/2025	22:59:48	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Box.SFT.AppUsers"		
1/31/2025	22:04:00	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"rs-ora-np-01.Contributor"		
1/31/2025	22:03:25	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"rs-ora-np-01.Owner.RBAC"		
1/31/2025	22:03:25	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"iRetiredev"		
1/31/2025	22:03:21	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"iRetireTest"		
1/31/2025	22:02:39	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"iRetireProd"		
1/31/2025	22:01:52	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"iRetireStage"		
1/31/2025	21:19:19	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/31/2025	21:18:28	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/31/2025	21:17:23	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/31/2025	21:15:41	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/31/2025	20:57:08	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/31/2025	20:56:56	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/31/2025	20:17:49	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-18]@opm.gov	"OCIO-STAMP-Users"		
1/31/2025	20:17:02	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/31/2025	20:16:08	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/31/2025	19:17:56	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"cto-digitalservices-np-01.Contributor.RBAC"		
1/31/2025	18:05:27	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/31/2025	17:54:25	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-8]@opm.gov	"OCIO-STAMP-Users"		
1/31/2025	17:50:27	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	Amanda.Scales@opm.gov	"OCIO-STAMP-Users"		
1/31/2025	17:39:53	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/31/2025	17:39:23	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/31/2025	17:28:22	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/31/2025	17:27:10	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/31/2025	17:26:54	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/31/2025	16:57:30	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/31/2025	16:55:41	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/31/2025	16:38:03	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/31/2025	16:37:59	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/31/2025	16:36:51	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/31/2025	16:36:38	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/31/2025	14:25:05	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"GHEC-OPM-OCIO-BAS-PAPS-USALearning-Architects"		
1/31/2025	14:24:30	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"GHEC-OPM-OCIO-BAS-PAPS-USALearning-Members"		
1/31/2025	14:23:51	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"GHEC-OPM-OCIO-BAS-PAPS-USALearning-Members"		
1/31/2025	14:23:50	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"OPM-GHEC-User-Read"		
1/31/2025	14:23:37	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-2]@opm.gov	"GHEC-OPM-OD-Members"		
1/31/2025	14:23:35	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"GHEC-OPM-OCIO-BAS-PAPS-USALearning-Members"		
1/31/2025	14:23:12	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"GHEC-OPM-OCIO-CTO-Members"		
1/31/2025	14:23:11	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"OPM-GHEC-User-Read"		
1/31/2025	14:23:07	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"GHEC-OPM-OCIO-BAS-PAPS-USALearning-Architects"		
1/31/2025	14:22:53	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"GHEC-OPM-OCIO-BAS-PAPS-USALearning-Members"		
1/31/2025	14:22:17	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"GHEC-OPM-OCIO-BAS-PAPS-USALearning-Members"		
1/31/2025	14:22:14	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"GHEC-OPM-OCIO-CTO-Members"		
1/31/2025	14:22:13	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"OPM-GHEC-User-Read"		
1/31/2025	14:22:05	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"GHEC-OPM-OCIO-BAS-PAPS-USALearning-DevOps"		
1/31/2025	14:21:38	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-5]@opm.gov	"GHEC-OPM-OD-Members"		
1/31/2025	14:21:34	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"GHEC-OPM-OCIO-BAS-PAPS-USALearning-DevOps"		
1/31/2025	14:21:31	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"GHEC-OPM-OCIO-BAS-PAPS-USALearning-DevOps"		
1/31/2025	14:21:30	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-3]@opm.gov	"GHEC-OPM-OD-Members"		
1/31/2025	14:21:26	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"GHEC-OPM-OCIO-BAS-PAPS-USALearning-Members"		
1/31/2025	14:21:25	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"OPM-GHEC-User-Read"		
1/31/2025	14:20:38	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"GHEC-OPM-OCIO-BAS-PAPS-USALearning-Members"		
1/31/2025	14:20:29	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"GHEC-OPM-OCIO-BAS-PAPS-USALearning-DevOps"		
1/31/2025	14:20:19	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"GHEC-OPM-OCIO-CTO-Members"		
1/31/2025	14:20:18	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"OPM-GHEC-User-Read"		
1/31/2025	14:17:28	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"GHEC-OPM-OCIO-BAS-PAPS-USALearning-Owners"		
1/31/2025	14:16:56	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"GHEC-OPM-OCIO-BAS-PAPS-USALearning-Owners"		
1/31/2025	14:16:39	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"GHEC-OPM-OCIO-BAS-PAPS-USALearning-Owners"		
1/31/2025	10:01:37	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-14]@opm.gov	"AZ.OPM.KnowBe4.User"		
1/31/2025	9:59:50	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/31/2025	9:59:46	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/31/2025	9:59:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
1/31/2025	9:59:17	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
1/31/2025	9:58:52	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-10]@opm.gov	"Az.OPM.LearningConnection.Prod.User"		
1/31/2025	9:56:25	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
1/31/2025	9:55:30	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		

Date (UTC)	Time	Service	Category	Activity	ActorDisplayName	Target1UserPrincipalName	Target1ModifiedProperty2NewValue		
1/31/2025	9:55:20	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-10]@opm.gov	"AZ.OPM.KnowBe4.User"		
1/31/2025	9:55:17	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-14]@opm.gov	"Az.OPM.LearningConnection.Prod.User"		
1/31/2025	5:16:13	Core Directory	UserManagement	Delete user	Azure AD Identity Governance - Directory Management	[PII]			
2/1/2025	5:07:36	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/1/2025	5:07:35	Core Directory	UserManagement	Update user	Azure AD Identity Governance - Directory Management	[PII]	"AccountEnabled"		
2/1/2025	5:07:35	Core Directory	UserManagement	Disable account	Azure AD Identity Governance - Directory Management	[PII]	"AccountEnabled"		
2/1/2025	5:06:57	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/1/2025	5:06:56	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/1/2025	5:06:55	Core Directory	UserManagement	Update user	Azure AD Identity Governance - Directory Management	[PII]	"AccountEnabled"		
2/1/2025	5:06:55	Core Directory	UserManagement	Disable account	Azure AD Identity Governance - Directory Management	[PII]	"AccountEnabled"		
2/2/2025	10:09:27	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/2/2025	10:07:44	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/3/2025	23:11:55	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"OCIO-STAMP-Users"		
2/3/2025	20:06:03	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/3/2025	20:04:56	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/3/2025	20:04:03	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/3/2025	20:03:11	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/3/2025	20:02:43	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/3/2025	20:02:20	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/3/2025	20:01:57	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/3/2025	19:52:12	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/3/2025	17:03:58	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/3/2025	17:03:37	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/3/2025	17:02:41	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/3/2025	17:01:59	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/3/2025	15:20:15	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs.usadata.data.stusasprd001.blob.mod"		
2/3/2025	15:19:15	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs.usadata.data.stusasnp.blob.mod"		
2/3/2025	15:18:28	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs.usadata.d.data.blob.mod"		
2/3/2025	15:17:06	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usad-p-001.StorageBlobMod.RBAC"		
2/3/2025	15:16:53	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usad-qa-001.StorageBlobMod.RBAC"		
2/3/2025	15:16:20	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usad-dev-001.StorageBlobMod.RBAC"		
2/3/2025	15:11:22	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"az.databrx.data.engineer.dtt.postal.prd"		
2/3/2025	15:11:19	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"az.databrx.data.engineer.dtt.postal.prd"		
2/3/2025	15:11:17	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"az.databrx.data.engineer.dtt.postal.prd"		
2/3/2025	15:09:19	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"az.databrx.data.analyst.ehri"		
2/4/2025	23:18:09	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
2/4/2025	23:15:19	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
2/4/2025	23:13:21	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Box.SFT.AppUsers"		
2/4/2025	23:12:57	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	22:59:23	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	22:36:37	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	22:18:41	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	22:18:33	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	21:57:55	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
2/4/2025	21:57:46	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
2/4/2025	21:36:53	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"az.janus.backend.prod.Users"		
2/4/2025	21:17:20	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
2/4/2025	21:16:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
2/4/2025	21:12:47	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"az.janus.frontend.prod.Users"		
2/4/2025	20:03:05	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usad-qa-001.Contributor.RBAC"		
2/4/2025	20:02:30	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usad-dev-001.Contributor.RBAC"		
2/4/2025	19:58:47	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
2/4/2025	19:58:33	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
2/4/2025	19:37:02	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
2/4/2025	19:36:48	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
2/4/2025	19:29:53	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.SharePoint-Admin"		
2/4/2025	18:58:45	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	18:58:01	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	18:55:26	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	18:55:17	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	18:40:06	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	17:40:53	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Box.SFT.AppUsers"		
2/4/2025	17:40:22	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	17:39:28	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Box.SFT.AppUsers"		
2/4/2025	17:35:37	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"HI – FEDVIP – Carrier Communications"		
2/4/2025	17:01:19	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management				
2/4/2025	16:59:56	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management				
2/4/2025	15:39:57	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management		"az.databrx.data.engineer.ehri.qa"		
2/4/2025	14:39:39	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
2/4/2025	14:39:20	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-15]@opm.gov	"AZ.OPM.KnowBe4.User"		
2/4/2025	14:38:50	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-12]@opm.gov	"AZ.OPM.KnowBe4.User"		
2/4/2025	14:38:25	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-11]@opm.gov	"AZ.OPM.KnowBe4.User"		
2/4/2025	14:35:53	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
2/4/2025	14:29:21	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-12]@opm.gov	"Az.OPM.LearningConnection.Prod.User"		
2/4/2025	14:29:20	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
2/4/2025	14:28:07	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
2/4/2025	14:25:58	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-15]@opm.gov	"Az.OPM.LearningConnection.Prod.User"		
2/4/2025	14:25:22	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-11]@opm.gov	"Az.OPM.LearningConnection.Prod.User"		
2/4/2025	13:48:11	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	13:37:04	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	13:16:26	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Apptio.Cloudability.User"		
2/4/2025	12:11:19	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"eid-eopf-helpdesk-footprints-apppxy-users"		
2/4/2025	10:19:59	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:19:48	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:19:48	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:19:41	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:19:24	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:19:14	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:19:13	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:19:13	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:18:58	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:18:54	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:18:40	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:18:25	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:18:11	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:17:57	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:17:54	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:17:33	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:17:18	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:17:12	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:17:10	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:17:06	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:17:03	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:16:55	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:16:55	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:16:54	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:16:51	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:16:28	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:16:20	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:16:15	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:15:56	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:15:54	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:15:49	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:15:29	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:15:20	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:15:16	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/4/2025	10:15:12	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/5/2025	20:59:51	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"rg-ocio-cyber-cprm-ai-np.CogServicesContributor"		
2/5/2025	20:57:56	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"rg-ocio-cyber-cprm-ai-np.Contributor"		
2/5/2025	19:22:45	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usaj-np-001.SubContributor"		
2/5/2025	19:22:45	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usaj-np-001.SubContributor"		
2/5/2025	19:21:42	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-sfs-np-001.Contributor.RBAC"		

Date (UTC)	Time	Service	Category	Activity	ActorDisplayName	Target1UserPrincipalName	Target1ModifiedProperty2NewValue		
2/5/2025	19:21:38	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-sfs-np-001.Contributor.RBAC"		
2/5/2025	19:07:16	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-sfs-p-001.Contributor.RBAC"		
2/5/2025	19:07:06	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-sfs-p-001.Contributor.RBAC"		
2/5/2025	19:05:35	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usal-p-001.Contributor.RBAC"		
2/5/2025	19:04:55	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usal-np-001.Contributor.RBAC"		
2/5/2025	19:03:45	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usaj-p-001.Contributor"		
2/5/2025	19:03:05	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usaj-np-001.Contributor.RBAC"		
2/5/2025	19:03:02	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usaj-np-001.Contributor.RBAC"		
2/5/2025	18:16:58	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/5/2025	18:16:57	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/5/2025	18:16:47	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/5/2025	18:16:45	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/5/2025	18:16:44	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/5/2025	18:16:44	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/5/2025	18:16:44	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/5/2025	18:16:44	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/5/2025	18:16:44	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/5/2025	18:16:44	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/5/2025	18:16:23	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/5/2025	18:16:20	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/5/2025	18:16:19	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/5/2025	18:16:19	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/5/2025	18:16:04	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/5/2025	18:16:03	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/5/2025	15:07:36	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"PPCOEToolkitUsers"		
2/5/2025	14:15:46	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"cdm dbaas scuba"		
2/5/2025	14:15:45	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"cdm dbaas scuba"		
2/5/2025	14:15:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"cdm dbaas scuba"		
2/5/2025	14:15:29	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"cdm dbaas scuba"		
2/5/2025	14:15:29	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"cdm dbaas scuba"		
2/5/2025	14:14:58	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"cdm dbaas cyhy "		
2/5/2025	14:14:58	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"cdm dbaas cyhy "		
2/5/2025	14:14:57	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"cdm dbaas cyhy "		
2/5/2025	14:14:56	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/5/2025	14:14:56	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/5/2025	14:14:55	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/5/2025	14:14:55	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/5/2025	14:14:49	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"cdm dbaas cyhy "		
2/5/2025	14:14:48	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"cdm dbaas cyhy "		
2/5/2025	14:14:48	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"cdm_dbaas_cyhy "		
2/5/2025	14:14:30	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/5/2025	14:14:27	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/5/2025	14:14:25	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/5/2025	14:14:25	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/5/2025	14:14:25	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/5/2025	14:14:25	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/5/2025	14:14:25	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/5/2025	14:14:25	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/5/2025	14:14:25	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/5/2025	14:14:24	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/6/2025	21:56:32	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/6/2025	21:55:23	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/6/2025	19:48:28	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
2/6/2025	19:39:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
2/6/2025	19:00:00	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/6/2025	18:58:38	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/6/2025	18:45:40	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/6/2025	18:38:47	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/6/2025	17:59:34	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
2/6/2025	17:55:56	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
2/6/2025	12:13:12	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"eid-eopf-helpdesk-footprints-apppxy-users"		
2/6/2025	11:44:29	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/6/2025	11:43:42	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/6/2025	10:29:24	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/6/2025	10:29:01	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/6/2025	10:28:49	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/6/2025	10:28:37	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/6/2025	10:27:53	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/6/2025	10:27:35	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/6/2025	10:27:28	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/6/2025	10:27:26	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/6/2025	10:27:18	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/6/2025	10:27:10	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/6/2025	10:27:05	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/6/2025	10:26:02	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/6/2025	10:25:51	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/6/2025	10:25:46	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/6/2025	10:25:44	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/6/2025	10:25:43	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/7/2025	21:11:52	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.B2B-DOJ-Collaborators"		
2/7/2025	21:11:50	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.B2B-DOJ-Collaborators"		
2/7/2025	20:44:41	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"rs-janusrc-p-001.Reader"		
2/7/2025	20:38:48	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.B2B-DOJ-Collaborators"		
2/7/2025	20:38:16	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.B2B-DOJ-Collaborators"		
2/7/2025	19:59:33	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"az.databrx.data.analyst.usadata.prod"		
2/7/2025	19:59:10	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"az.databrx.data.analyst.usadata.dev"		
2/7/2025	19:38:08	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"rs-janusrc-p-001.Reader"		
2/7/2025	19:28:17	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.AAD.GlobalReader"		
2/7/2025	18:10:50	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Box.SFT.AppUsers"		
2/7/2025	18:08:57	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/7/2025	17:50:29	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"GHEC-OPM-OCIO-FITBS-HRSITPMO-USAP-DevOps"		
2/7/2025	16:10:35	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usal-np-001.Owner.RBAC"		
2/7/2025	15:05:18	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"az.databrx.data.analyst.usadata.dev"		
2/7/2025	15:05:02	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.Exchange-Admin"		
2/7/2025	15:05:00	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.Exchange-Admin"		
2/7/2025	15:03:18	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"az.databrx.data.scientist.usadata"		
2/7/2025	15:01:14	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"az.databrx.data.analyst.ehri"		
2/7/2025	14:56:29	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"az.databrx.data.engineer.dtt.postal.prd"		
2/7/2025	14:56:23	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"az.databrx.data.engineer.dtt.postal.prd"		
2/7/2025	14:56:23	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"az.databrx.data.engineer.dtt.postal.prd"		
2/7/2025	14:05:45	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[OPM-4]@opm.gov			
2/7/2025	14:03:18	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[OPM-4]@opm.gov			
2/7/2025	13:39:55	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"ocio-cyber-p-001.Reader.RBAC"		
2/7/2025	13:39:54	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"rg-AzLogs-p-001.Contributor.RBAC"		
2/7/2025	13:39:53	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"rg-AzLogs-p-001.Reader"		
2/7/2025	13:39:52	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.rg-cyber-playbooks-p-001.Contributor"		
2/7/2025	13:39:51	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.Purview-IRM-Analysts"		
2/7/2025	13:39:51	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.Global.Reader.RBAC"		
2/7/2025	13:39:50	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.Security.Reader"		
2/7/2025	13:35:54	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/7/2025	13:35:53	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/7/2025	13:35:53	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/7/2025	13:35:52	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/7/2025	13:35:51	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/7/2025	13:35:50	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/7/2025	13:35:50	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/7/2025	2:31:26	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov	"hrs-opmdata-qa-001.SubContributor.RBAC"		
2/7/2025	2:31:22	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-2]@opm.gov	"hrs-opmdata-qa-001.SubContributor.RBAC"		
2/7/2025	2:29:04	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-2]@opm.gov	"hrs-opmdata-qa-001.Reader.RBAC"		
2/7/2025	2:28:59	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov	"hrs-opmdata-qa-001.Reader.RBAC"		
2/7/2025	2:24:17	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[OPM-2]@opm.gov			
2/7/2025	2:24:16	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov			

Date (UTC)	Time	Service	Category	Activity	ActorDisplayName	Target1UserPrincipalName	Target1ModifiedProperty2NewValue		
2/7/2025	2:06:10	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[OPM-2]@opm.gov			
2/7/2025	2:06:10	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov			
2/7/2025	2:04:58	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[OPM-2]@opm.gov			
2/7/2025	2:04:58	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov			
2/8/2025	23:38:41	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usal-np-001.FullContributor.RBAC"		
2/8/2025	11:08:17	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
2/8/2025	10:59:02	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
2/8/2025	4:16:07	Core Directory	UserManagement	Delete user	Azure AD Identity Governance - Directory Management	[PII]			
2/9/2025	4:07:58	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/9/2025	4:07:34	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	21:49:55	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	21:48:28	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	21:48:27	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	21:45:18	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	20:12:35	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Apptio.Cloudability.User"		
2/10/2025	20:12:33	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Apptio.Cloudability.User"		
2/10/2025	20:01:30	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.Intune-Admin"		
2/10/2025	19:59:04	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"ocio-itops-p-001.Contributor.RBAC"		
2/10/2025	18:47:30	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	18:47:24	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	18:47:24	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	18:47:23	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	18:47:23	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	17:33:43	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	17:33:42	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	17:33:42	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	17:33:41	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	17:33:41	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	17:33:40	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	17:33:39	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	17:33:38	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	17:33:37	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	17:33:36	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	17:33:36	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	17:33:35	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	17:33:34	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	17:33:34	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	17:32:38	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	17:32:37	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	17:32:36	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	17:32:36	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	17:32:35	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	16:42:40	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.USAStaffingLMS.Prod.User"		
2/10/2025	16:00:18	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
2/10/2025	15:58:32	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	15:38:19	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
2/10/2025	15:36:13	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	14:47:05	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Apptio.Cloudability.User"		
2/10/2025	14:46:57	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Apptio.Cloudability.User"		
2/10/2025	14:46:57	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Apptio.Cloudability.User"		
2/10/2025	14:46:52	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Apptio.Cloudability.User"		
2/10/2025	14:40:01	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usal-p-001.Full.Owner.RBAC"		
2/10/2025	14:39:04	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.USAStaffingLMS.Prod.User"		
2/10/2025	14:38:50	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usal-np-001.Full.Owner.RBAC"		
2/10/2025	14:26:39	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-usaj-p-001.Full.Owner.RBAC"		
2/10/2025	5:13:54	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	5:06:51	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	5:06:50	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	5:06:47	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	5:06:46	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	5:06:05	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	5:06:04	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	5:05:54	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	5:05:54	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	5:05:20	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	5:05:19	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	4:09:40	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	4:07:57	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	4:07:51	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/10/2025	4:07:51	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/11/2025	22:13:08	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/11/2025	22:11:34	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/11/2025	22:08:57	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/11/2025	22:08:57	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/11/2025	22:08:23	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/11/2025	22:07:56	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/11/2025	22:07:39	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/11/2025	22:05:22	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/11/2025	22:02:22	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/11/2025	20:50:53	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"OCIO-STAMP-Users"		
2/11/2025	20:06:00	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.BMS.Admin.NP"		
2/11/2025	20:05:55	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.BMS.Admin.NP"		
2/11/2025	20:05:55	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.BMS.Admin.NP"		
2/11/2025	20:05:55	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.BMS.Admin.NP"		
2/11/2025	20:05:54	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.BMS.Admin.NP"		
2/11/2025	20:05:53	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.BMS.Admin.NP"		
2/11/2025	20:05:51	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.BMS.Admin.NP"		
2/11/2025	16:14:08	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"HRS – LAB – WIC Collaboration"		
2/11/2025	14:41:14	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"OCIO-STAMP-Users"		
2/11/2025	14:38:51	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/11/2025	14:24:34	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Box.SFT.AppUsers"		
2/11/2025	14:24:07	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/11/2025	14:03:03	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.CLDCentral.Prod.User"		
2/12/2025	20:10:03	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
2/12/2025	20:08:13	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/12/2025	20:07:56	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/12/2025	20:07:50	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
2/12/2025	20:06:58	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
2/12/2025	20:06:46	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/12/2025	20:05:15	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
2/12/2025	20:05:11	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/12/2025	19:49:00	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/12/2025	19:45:27	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/12/2025	19:27:13	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/12/2025	19:27:03	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/12/2025	19:08:27	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/12/2025	19:08:15	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/12/2025	19:07:33	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/12/2025	19:07:14	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/12/2025	18:08:56	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/12/2025	18:08:41	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
2/12/2025	18:07:43	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/12/2025	18:07:34	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/12/2025	18:07:24	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/12/2025	18:06:59	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
2/12/2025	18:06:52	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/12/2025	18:05:27	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[PII]			
2/12/2025	16:56:22	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"DFS Development"		
2/12/2025	16:42:18	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"DFS Testing"		
2/12/2025	16:13:10	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-opf-p-001.Reader.RBAC"		
2/12/2025	16:12:38	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"hrs-opf-np-001.Reader.RBAC"		
2/12/2025	16:07:11	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		

Date (UTC)	Time	Service	Category	Activity	ActorDisplayName	Target1UserPrincipalName	Target1ModifiedProperty2NewValue		
2/12/2025	16:05:20	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
2/12/2025	15:57:42	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.CLDCentral.Dev.User"		
2/12/2025	15:56:56	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.CLDCentral.Prod.User"		
2/12/2025	15:56:06	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.CLDCentral.Test.User"		
2/12/2025	13:54:44	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"CIITAR Application Users"		
2/12/2025	11:48:36	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"Az.OPM.LearningConnection.Prod.User"		
2/12/2025	11:46:19	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.KnowBe4.User"		
2/12/2025	0:06:57	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[OPM-2]@opm.gov			
2/12/2025	0:06:53	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov			
2/12/2025	0:06:52	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[OPM-4]@opm.gov			
2/12/2025	0:06:52	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[OPM-6]@opm.gov			
2/12/2025	0:06:52	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	Amanda.Scales@opm.gov			
2/12/2025	0:06:52	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[OPM-3]@opm.gov			
2/12/2025	0:06:52	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[OPM-5]@opm.gov			
2/12/2025	0:06:51	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[OPM-4]@opm.gov			
2/12/2025	0:06:51	Core Directory	GroupManagement	Remove member from group	Azure AD Identity Governance - Directory Management	[OPM-7]@opm.gov			
2/13/2025	15:14:05	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"eid-usas-footprints-apppxy-users"		
2/13/2025	15:14:03	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"eid-usas-footprints-apppxy-users"		
2/13/2025	13:34:23	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Apptio.Cloudability.User"		
2/13/2025	13:34:19	Core Directory	GroupManagement	Add member to group	Azure AD Identity Governance - Directory Management	[PII]	"AZ.OPM.Apptio.Cloudability.User"		

Employee Name	System Name	Date Created	Date Removed	Admin Access (Yes/No?)	Login (Yes/No?)
Amanda Scales	OPM Data : Azure Databricks Admin + NP / PRD Azure Subscriptions [OPMData / USADATA]	2/3/2025		Yes	No
Amanda Scales	USA Staffing Core + Admin Portal - DEV/TST/STG/TRN/PRD	1/20/2025		Yes	Yes Last Login 2025-02-28
Amanda Scales	USA Performance - U.S. Office of Personnel Management	1/20/2025	N/A	Yes	No
Amanda Scales	USA Performance - Office of the Director	1/31/2025	N/A	Yes	No
Amanda Scales	FEHB - Federal Employees Health Benefits	2/3/2025		Yes	No
Amanda Scales	PSHB HBDP - Postal Service Health Benefits Data Platform	2/3/2025		Yes	No
Charles Ezell	OPM Data : Connect Platform (Az.opm.entraID.efficiencyorg.admin + Az.cio.entraID.PowerBIAdmin)	1/20/2025		Yes	No
Greg Hogan	OPM Data : Azure Databricks Admin + NP / PRD Azure Subscriptions [OPMData / USADATA]	1/28/2025		Yes	No
Greg Hogan	OPM Data : Connect Platform (Az.opm.entraID.efficiencyorg.admin + Az.cio.entraID.PowerBIAdmin)	1/20/2025		Yes	No
Greg Hogan	USA Performance - U.S. Office of Personnel Management	1/20/2025	N/A	Yes	Yes
Greg Hogan	FEHB - Federal Employees Health Benefits	1/28/2025		Yes	No
Greg Hogan	PSHB HBDP - Postal Service Health Benefits Data Platform	1/30/2025		Yes	No
OPM-10	USA Performance - Office of the Director	2/7/2025	N/A	Yes	No
OPM-11	USA Performance - Office of the Director	2/7/2025	N/A	Yes	No
OPM-12	USA Performance - Office of the Director	2/7/2025	N/A	Yes	No
OPM-13	USA Performance - Office of the Director	1/31/2025	N/A	Yes	No
OPM-14	USA Performance - Office of the Director	2/7/2025	N/A	Yes	No
OPM-15	USA Performance - Office of the Director	2/7/2025	N/A	Yes	No
OPM-16	USA Performance - Office of the Director	1/31/2025	N/A	Yes	No
OPM-17	USA Performance - Office of the Director	1/31/2025	N/A	Yes	No
OPM-18	USA Performance - Office of the Director	1/24/2025	N/A	Yes	No
OPM-2	OPM Data : Azure Databricks Admin + NP / PRD Azure Subscriptions [OPMData / USADATA]	1/28/2025		Yes	No
OPM-2	OPM Data : Connect Platform (Az.opm.entraID.efficiencyorg.admin + Az.cio.entraID.PowerBIAdmin)	1/28/2025		Yes	No
OPM-2	OPM Data : Electronic Official Personnel Folder (eOPF) - DEV/TST/QA/TRN/PRD	1/28/2025	2/6/2025	No	No - never completed User registraion
OPM-2	OPM Data : Enterprise Human Resources Integration (EHRI) - Dev/TST/QA/PRD	1/28/2025	2/6/2025	No	No - never completed User registraion
OPM-2	FEHB - Federal Employees Health Benefits	1/28/2025		Yes	No
OPM-2	PSHB HBDP - Postal Service Health Benefits Data Platform	1/28/2025		Yes	No
OPM-2h	USA Performance - U.S. Office of Personnel Management	1/28/2025	N/A	Yes	No
OPM-3	OPM Data : Connect Platform (Az.opm.entraID.efficiencyorg.admin + Az.cio.entraID.PowerBIAdmin)	1/20/2025		Yes	No
OPM-3	USA Performance - U.S. Office of Personnel Management	1/20/2025	N/A	Yes	No
OPM-4	USA Performance - U.S. Office of Personnel Management	1/28/2025	N/A	Yes	No
OPM-4	OPM Data : Azure Databricks Admin + NP / PRD Azure Subscriptions [OPMData / USADATA]	1/28/2025		Yes	No
OPM-4	OPM Data : Connect Platform (Az.opm.entraID.efficiencyorg.admin + Az.cio.entraID.PowerBIAdmin)	1/28/2025		Yes	No
OPM-4	OPM Data : Electronic Official Personnel Folder (eOPF) - DEV/TST/QA/TRN/PRD	1/28/2025	2/6/2025	No	No - never completed User registraion
OPM-4	OPM Data : Enterprise Human Resources Integration (EHRI) - Dev/TST/QA/PRD	1/28/2025	2/6/2025	No	No - never completed User registraion
OPM-4	FEHB - Federal Employees Health Benefits	1/28/2025		Yes	No
OPM-4	PSHB HBDP - Postal Service Health Benefits Data Platform	1/28/2025		Yes	No
OPM-5	OPM Data : Azure Databricks Admin + NP / PRD Azure Subscriptions [OPMData / USADATA]	1/28/2025		Yes	No
OPM-5	OPM Data : Connect Platform (Az.opm.entraID.efficiencyorg.admin + Az.cio.entraID.PowerBIAdmin)	1/20/2025		Yes	No
OPM-5	USA Performance - U.S. Office of Personnel Management	1/20/2025	N/A	Yes	No
OPM-5	FEHB - Federal Employees Health Benefits	1/28/2025		Yes	No
OPM-5	PSHB HBDP - Postal Service Health Benefits Data Platform	1/30/2025		Yes	No
OPM-6	OPM Data : Azure Databricks Admin + NP / PRD Azure Subscriptions [OPMData / USADATA]	1/28/2025		Yes	Yes
OPM-6	OPM Data : Connect Platform (Az.opm.entraID.efficiencyorg.admin + Az.cio.entraID.PowerBIAdmin)	1/28/2025		Yes	No
OPM-6	OPM Data : Electronic Official Personnel Folder (eOPF) - DEV/TST/QA/TRN/PRD	1/28/2025	2/6/2025	No	No - never completed User registraion
OPM-6	OPM Data : Enterprise Human Resources Integration (EHRI) - Dev/TST/QA/PRD	1/28/2025	2/6/2025	No	No - never completed User registraion
OPM-6	USA Staffing Core + Admin Portal - DEV/TST/STG/TRN/PRD	1/28/2025	2/24/2025	Yes	Yes Last Login 2025-2-24
OPM-6	USA Performance - U.S. Office of Personnel Management	1/28/2025	N/A	Yes	No
OPM-6	FEHB - Federal Employees Health Benefits	1/28/2025		Yes	No
OPM-6	PSHB HBDP - Postal Service Health Benefits Data Platform	1/28/2025		Yes	No
OPM-7	USA Performance - U.S. Office of Personnel Management	1/20/2025	N/A	Yes	No
OPM-7	USA Staffing Core + Admin Portal - DEV/TST/STG/TRN/PRD	1/20/2025		Yes	Yes Last Login 2024-11-07
OPM-8	OPM Data : Azure Databricks Admin + NP / PRD Azure Subscriptions [OPMData / USADATA]	2/3/2025		Yes	No
OPM-8	USA Staffing Core + Admin Portal - DEV/TST/STG/TRN/PRD	2/3/2025		Yes	Yes Last Login 2025-02-23
OPM-8	USA Performance - Office of the Director	1/31/2025	N/A	Yes	No
OPM-8	FEHB - Federal Employees Health Benefits	2/3/2025		Yes	No
OPM-8	PSHB HBDP - Postal Service Health Benefits Data Platform	2/3/2025		Yes	No
OPM-9	OPM Data : Azure Databricks Admin + NP / PRD Azure Subscriptions [OPMData / USADATA]	2/4/2025		Yes	No
OPM-9	USA Performance - Office of the Director	1/31/2025	N/A	Yes	No
OPM-9	FEHB - Federal Employees Health Benefits	2/4/2025		Yes	No
OPM-9	PSHB HBDP - Postal Service Health Benefits Data Platform	2/3/2025		Yes	No

From: Quinn, Quadrina L.
To: Scales, Amanda D.; OPM-5 Hogan, Greg; OPM-7 OPM-3 Ezell, Charles E.
Cc: Walicek, Wayne; Fordham, Marshall T.; Price, MC; Curtis, Teresa A.
Subject: USAJOBS admin accounts
Date: Monday, January 20, 2025 6:41:52 PM
Attachments: image001.png

Hi all,

We have created administrator accounts with super user permissions for the USAJOBS admin systems below. The Web Admin system utilizes OPM single-sign-on (EntraID) to automatically log you in. In Agency Talent Portal you can use PIV or login.gov to authenticate into the system. Please let me know if you have any questions or issues with accessing these sites!

USAJOBS Web Admin
https://webadmin.usajobs.gov (production)
https://webadmin.uat.usajobs.gov (user acceptance testing environment)
https://webadmin.test.usajobs.gov (test environment)
https://webadmin.dev.usajobs.gov (development environment)

USAJOBS Agency Talent Portal
https://agencyportal.usajobs.gov/ (production)
https://agencyportal.uat.usajobs.gov (user acceptance testing environment)
https://agencyportal.test.usajobs.gov (test environment)
https://agencyportal.dev.usajobs.gov (development environment)

Thanks,
Quadrina Quinn
Supervisory IT Specialist
U.S. Office of Personnel Management
Office of the Chief Information Officer
c: (202) [redacted]
[redacted]@opm.gov
OPM.gov

Follow us on LinkedIn | Twitter | YouTube

From: Quinn, Quadrina L.
To: OPM-6 OPM-2 OPM-4
Cc: Walicek, Wayne; Curtis, Teresa A.; Price, MC; Fordham, Marshall T.; Sarazine, Luke W.; Scales, Amanda
Subject: Access to USAJOBS
Date: Tuesday, January 28, 2025 4:29:25 PM
Attachments: image001.png

Hi all,

The requested access, permissions and documentation are below. Please let us know if you have any questions or issues!

- Code read and write permissions
  - Code read and write permissions will be granted via GitHub. The USAJOBS repositories can be located here. If you have any issues please contact Christopher Inman
- Deploy ability Octopus deploy
  - Deploy ability in Octopus Deploy – If you have any issues please contact Christopher Inman.
- Monitoring dashboards (e.g. displaying success rates, volume of traffic)
  - USAJ Production Azure Application Insights Dashboard
  - USAJ UAT Azure Application Insights
  - USAJ Test Azure Application Insights
  - USAJ DEV Azure Application Insights
- Documentation (e.g. test and deploy instructions, system diagrams)
  - USAJOBS code repository readme
  - USAJOBS infrastructure readme
  - USAJOBS system diagram
- The on-call rotation for the system
  - Tony Dalton - 202-[redacted] (Devops/system administration)
  - James Moon - 478-[redacted] (DBA)
- Names of all engineers deeply familiar with the system
  - Keith Lawrence – Systems Architect
  - Saleim Abushanab – Lead Developer
  - Jacob Riley – Lead Developer
  - Wayne Kaye – Lead Developer
  - Marshall Fordham – Supervisor
  - Quadrina Quinn – Supervisor
  - Luke Sarazine – Supervisor
- Ability to access the system as a regular user
  - USAJOBS.gov accounts will need to be self-registered.
- Ability to access the system as an admin user.
  - USAJOBS Web Admin accounts created with super user permissions. The Web Admin system utilizes OPM single-sign-on (EntraID) to automatically log you in
  - USAJOB Agency Talent Portal account invites sent. You can use PIV or login.gov to authenticate into the system.

Thanks,

Quadrina Quinn
Supervisory IT Specialist
U.S. Office of Personnel Management
Office of the Chief Information Officer
c: (202) [redacted]
[redacted]@opm.gov
OPM.gov

Follow us on LinkedIn | Twitter | YouTube

From: Curtis, Teresa A.
To: Hurst, Corey D.; Price, MC
Cc: Walicek, Wayne; Corum, Brice M.; DesCombes, Daniel; Parham, Lee; Sarazine, Luke W.
Subject: Re: urgent request from political tech staff
Date: Thursday, January 30, 2025 10:28:47 AM
Attachments: Outlook-t4jdpy0h.png

Yes - The request was from the Acting Director to MC on Monday January 20th to add these people to the system as admins.

Teresa Curtis
Deputy Associate Chief Information Officer
U.S. Office of Personnel Management
Office of the Chief Information Officer, Federal Information Technology Business Solutions
c: (816) [redacted]
[redacted]@opm.gov
OPM.gov

From: Hurst, Corey D. <[redacted]@opm.gov>
Sent: Thursday, January 30, 2025 8:37 AM
To: Price, MC <[redacted]@opm.gov>; Curtis, Teresa A. <[redacted]@opm.gov>
Cc: Walicek, Wayne <[redacted]@opm.gov>; Corum, Brice M. <[redacted]@opm.gov>; DesCombes, Daniel <[redacted]@opm.gov>; Parham, Lee <[redacted]@opm.gov>; Sarazine, Luke W. <[redacted]@opm.gov>
Subject: Re: urgent request from political tech staff

Good Morning MC/Teresa,

I can't seem to find the first request for the 6 individuals that we granted this access for. I'm thinking it was due to the 911-esque call we had that evening. Can you please confirm guidance/approval for the access for these folks from 1/20/25, for documentation purposes?

Individuals from the Political Team:

amanda.scales@opm.gov
OPM-5 @opm.gov
greg.hogan@opm.gov
OPM-7 @opm.gov
OPM-3 @opm.gov
charles.ezell@opm.gov

Thank you,

Corey Hurst
Supervisory IT Specialist
U.S. Office of Personnel Management
OCIO – HR Solutions IT PMO – USA Staffing
Office (Teams): 202-[redacted]
Cell: 478-[redacted]
[redacted]@opm.gov
OPM.gov

OPM U.S. Office of Personnel Management
Follow us on LinkedIn | Twitter | YouTube

From: Price, MC <[redacted]@opm.gov>
Sent: Tuesday, January 28, 2025 9:07 AM
To: Meck, Aaron R. [redacted]@opm.gov>; Boles, Jason R [redacted]@opm.gov>; Burke, Paul T. [redacted]@opm.gov>; Corum, Brice M. [redacted]@opm.gov>; Curtis, Teresa A. [redacted]@opm.gov>; Davis, Leslie B. <[redacted]@opm.gov>; Decker, DJ <[redacted]@opm.gov>; DesCombes, Daniel <[redacted]@opm.gov>; Eavenson, Keith W. <[redacted]@opm.gov>; Ezell, Phillip A. <[redacted]@opm.gov>; Fordham, Marshall T. <[redacted]@opm.gov>; Foster, Ozie L. <[redacted]@opm.gov>; Hurst, Corey D. <[redacted]@opm.gov>; Inman, Christopher M. <[redacted]@opm.gov>; Leski, David R. <[redacted]@opm.gov>; Mathews, Brian C. [redacted]@opm.gov>; Meck, Aaron R. <[redacted]@opm.gov>; Micko, Robert J. <[redacted]@opm.gov>; Parham, Lee <[redacted]@opm.gov>; Price, MC <[redacted]@opm.gov>; Quinn, Quadrina L. <[redacted]@opm.gov>; Raval, Divya <[redacted]@opm.gov>; Sarazine, Luke W. <[redacted]@opm.gov>; Shelton, Angela K. [redacted]@opm.gov>; Walicek, Wayne [redacted]@opm.gov>; Williams, Melanie [redacted]@opm.gov>; Williamson, Kim H. [redacted]@opm.gov>; Papp, David [redacted]@opm.gov>; Williams, Melanie [redacted]@opm.gov>
Subject: urgent request from political tech staff

Quadrina, Brice, Corey, Daniel, Ozie, Dave, Luke, Paul, others as needed.

We have already given several of the political devs/engineers comprehensive access to USAJOBS and USA Staffing, and local admin, Enterprise Github licenses, etc. Now we have 3 more individuals with the same requirement. We'll start with USAJOBS, USA Staffing, and eOPF/EHRI. USAP will be next, so might as well go ahead there. I will give them the leads to work with for these three and they will most likely reach out to discuss the bullets below (the how to's, along with the access).

The need to have access today, so please work through all the wickets, and Luke/Quadrina/Marshall, Brice/Daniel, Ozie, send them an intro message letting them know (please copy me).

OPM-6 @opm.gov
OPM-2 @opm.gov

OPM-4 @opm.gov

- Code read and write permissions
- Deploy ability Octopus deploy
- Monitoring dashboards (e.g. displaying success rates, volume of traffic)
- Documentation (e.g. test and deploy instructions, system diagrams)
- The on-call rotation for the system
- Names of all engineers deeply familiar with the system
- Names of all product/project managers deeply familiar with the system
- Ability to access the system as a regular user (e.g. hiring manager and onboarding user for USA Staffing)
- Ability to access the system as an admin user

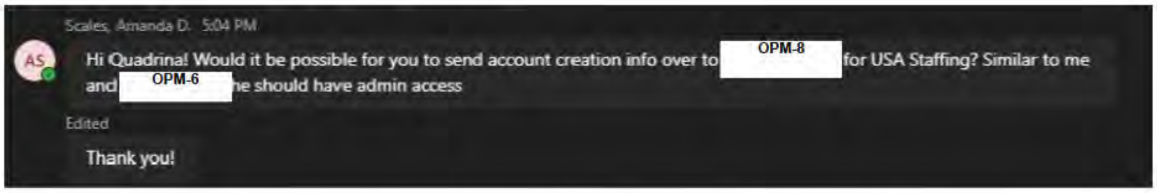
From: Price, MC
To: Hurst, Corey D.; Curtis, Teresa A.
Cc: Walicek, Wayne; Corum, Brice M.; DesCombes, Daniel
Subject: RE: USA Staffing Access Request - OPM-8 @opm.gov
Date: Monday, February 3, 2025 5:40:30 PM
Attachments: image001.png
image002.png

Approved.

From: Hurst, Corey D. <[redacted]@opm.gov>
Sent: Monday, February 3, 2025 5:32 PM
To: Price, MC[redacted]@opm.gov>; Curtis, Teresa A. <[redacted]@opm.gov>
Cc: Walicek, Wayne[redacted]@opm.gov>; Corum, Brice M. <[redacted]@opm.gov>; DesCombes, Daniel <[redacted]@opm.gov>
Subject: USA Staffing Access Request - OPM-8 @opm.gov
Importance: High

MC,

Please see below for the access request from Amanda Scales:



Scales, Amanda D. 5:04 PM

Hi Quadrina! Would it be possible for you to send account creation info over to OPM-8 for USA Staffing? Similar to me and OPM-6 he should have admin access

Edited

Thank you!

Please let me know as soon as you can if this is approved or not. I will be ready to take action once approval is received.

Corey Hurst

Supervisory IT Specialist

U.S. Office of Personnel Management

OCIO – HR Solutions IT PMO – USA Staffing

Office (Teams): 202-[redacted]

Cell: 478[redacted]

[redacted]@opm.gov

OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

Standard Form 50
Rev. 7/91
U.S. Office of Personnel Management
FPM Supp. 296-33, Subch. 4

NOTIFICATION OF PERSONNEL ACTION

1. Name (Last, First, Middle) OPM-7	2. Social Security Number [redacted]	3. Date of Birth [redacted]	4. Effective Date 01/20/2025

FIRST ACTION

5-A. Code 171	5-B. Nature of Action EXC APPT NTE 07/18/2025
5-C. Code H2L	5-D. Legal Authority REG 304.103.
5-E. Code	5-F. Legal Authority

SECOND ACTION

6-A. Code	6-B. Nature of Action
6-C. Code	6-D. Legal Authority
6-E. Code	6-F. Legal Authority

7. FROM: Position Title and Number

8. Pay Plan	9. Occ. Code	10. Grade or Level	11. Step or Rate	12. Total Salary	13. Pay Basis

12A. Basic Pay	12B. Locality Adj.	12C. Adj. Basic Pay	12D. Other Pay

14. Name and Location of Position's Organization

15. TO: Position Title and Number
EXPERT
PD: 6A39743

16. Pay Plan	17. Occ. Code	18. Grade or Level	19. Step or Rate	20. Total Salary/Award	21. Pay Basis
ED	0301	00	00	$0	WC

20A. Basic Pay	20B. Locality Adj.	20C. Adj. Basic Pay	20D. Other Pay
$0	$0	$0	$0

22. Name and Location of Position's Organization
OPM
OFC OF THE DIRECTOR

WASHINGTON DC

EMPLOYEE DATA

23. Veterans Preference: 1 (1 - None; 2 - 5 Point; 3 - 10 Point/Disability; 4 - 10 Point/Compensable; 5 - 10 Point/Other; 6 - 10 Point/Compensable/30%)

24. Tenure: 0 (0 - None; 1 - Permanent; 2 - Conditional; 3 - Indefinite)

25. Agency Use: TG

26. Veterans Preference for RIF: YES [✓ X NO]

27. FEGLI: A0 [redacted]

28. Annuitant Indicator: 9 NOT APPLICABLE

29. Pay Rate Determinant: 0

30. Retirement Plan: 4 [redacted]

31. Service Comp. Date (Leave): 01/20/2025

32. Work Schedule: F FULL TIME

33. Part-Time Hours Per Biweekly Pay Period

POSITION DATA

34. Position Occupied: 2 (1 - Competitive Service; 2 - Excepted Service; 3 - SES General; 4 - SES Career Reserved)

35. FLSA Category: E (E - Exempt; N - Nonexempt)

36. Appropriation Code: 41AA0

37. Bargaining Unit Status: 8888

38. Duty Station Code: 11-0010-001

39. Duty Station (City - County - State or Overseas Location): WASHINGTON DISTRICT OF COLUMBIA DC

40. Agency Data	41.	42.	43.	44.
10001		0000	33.94	CRITICAL-SENSITIVE (CS)/HIGH R

45. Remarks

```
APPOINTMENT AFFIDAVIT EXECUTED 01-20-2025
REASON FOR TEMPORARY APPOINTMENT:   TO PROVIDE A HIGH LEVEL OF EXPERTISE RELATIVE TO ISSUES WHICH HAVE A
 SIGNIFICANT IMPACT ON THE FORMULATION OF AGENCY GOALS AND OBJECTIVES TO THE OPM DIRECTOR.
CREDITABLE MILITARY SERVICE: NONE
PREVIOUS RETIREMENT COVERAGE:  NEVER COVERED
```

46. Employing Department or Agency: OPM

47. Agency Code: OM00

48. Personnel Office ID: 1000

49. Approval Date: 01/30/2025

50. Signature/Authentication and Title of Approving Official
ELECTRONICALLY SIGNED BY:
CARMEN GARCIA-WHITESIDE
CHIEF HUMAN CAPITAL OFFICER AND DIRECTOR OF OPM HR

APPOINTMENT AFFIDAVITS

Expert	01/20/2025
(Position to which Appointed)	*(Date Appointed)*

Office of Personnel Managemer	Office of the Director	Washington, D.C.
(Department or Agency)	*(Bureau or Division)*	*(Place of Employment)*

I, OPM-7 ____________________, do solemnly swear (or affirm) that--

A. OATH OF OFFICE

I will support and defend the Constitution of the United States against all enemies, foreign and domestic; that I will bear true faith and allegiance to the same; that I take this obligation freely, without any mental reservation or purpose of evasion; and that I will well and faithfully discharge the duties of the office on which I am about to enter. So help me God.

B. AFFIDAVIT AS TO STRIKING AGAINST THE FEDERAL GOVERNMENT

I am not participating in any strike against the Government of the United States or any agency thereof, and I will not so participate while an employee of the Government of the United States or any agency thereof.

C. AFFIDAVIT AS TO THE PURCHASE AND SALE OF OFFICE

I have not, nor has anyone acting in my behalf, given, transferred, promised or paid any consideration for or in expectation or hope of receiving assistance in securing this appointment.

OPM-7

Subscribed and sworn (or affirmed) before me this 20 day of January, 2025

at Washington DC
(City) (State)

[illegible]
(Signature of Officer)

(SEAL)

Acting Director
(Title)

Commission expires__________
(If by a Notary Public, the date of his/her Commission should be shown)

Note - If the appointee objects to the form of the oath on religious grounds, certain modifications may be permitted pursuant to the Religious Freedom Restoration Act. Please contact your agency's legal counsel for advice.

Acceptance of Uncompensated Services

I understand that I may be employed with the United States Office of Personnel Management (OPM) under the authority of 5 U.S.C. § 3109. Under certain circumstances, OPM may use this authority to employ experts or consultants with or without pay, provided that such personnel agree in advance in writing to waive any claims for compensation for those services.

I desire to offer my services to OPM. Accordingly, I agree to being appointed as an uncompensated employee of OPM; I understand that I will not receive any pay or any other form of compensation from OPM, the federal Government, or any other source for the services I render to OPM.

In addition, I hereby waive any and all claims I may have in the future against OPM and/or the federal Government on account of the services I render to OPM.

OPM-7

Signed:

Printed Name of Appointee: OPM-7 ____

Date: ____January 20, 2025__________________

Standard Form 50
Rev. 7/91
U.S. Office of Personnel Management
FPM Supp. 296-33, Subch. 4

NOTIFICATION OF PERSONNEL ACTION

1. Name (Last, First, Middle) OPM-8	2. Social Security Number [redacted]	3. Date of Birth [redacted]	4. Effective Date 01/20/2025

FIRST ACTION

5-A. Code 146	5-B. Nature of Action SES NONCAREER APPT
5-C. Code V4L	5-D. Legal Authority 5 U.S.C. 3394(A).
5-E. Code AWM	5-F. Legal Authority OPM MEMO DTD 1-20-2025

SECOND ACTION

6-A. Code	6-B. Nature of Action
6-C. Code	6-D. Legal Authority
6-E. Code	6-F. Legal Authority

7. FROM: Position Title and Number

15. TO: Position Title and Number
SENIOR ADVISOR TO THE DIRECTOR
PD: 6A37370

8. Pay Plan	9. Occ. Code	10. Grade or Level	11. Step or Rate	12. Total Salary	13. Pay Basis

12A. Basic Pay	12B. Locality Adj.	12C. Adj. Basic Pay	12D. Other Pay

16. Pay Plan	17. Occ. Code	18. Grade or Level	19. Step or Rate	20. Total Salary/Award	21. Pay Basis
ES	0301	00	00	$195,200.00	PA

20A. Basic Pay	20B. Locality Adj.	20C. Adj. Basic Pay	20D. Other Pay
$195,200.00	$0	$195,200.00	$0

14. Name and Location of Position's Organization

22. Name and Location of Position's Organization
OPM
OFC OF THE DIRECTOR
WASHINGTON DC

EMPLOYEE DATA

23. Veterans Preference: 1 (1 - None; 2 - 5 Point; 3 - 10-Point/Disability; 4 - 10-Point/Compensable; 5 - 10-Point/Other; 6 - 10-Point/Compensable/30%)

24. Tenure: 0 (0 - None; 1 - Permanent; 2 - Conditional; 3 - Indefinite)

25. Agency Use: MK

26. Veterans Preference for RIF: YES [✓ X] NO

27. FEGLI: B0 [redacted]

28. Annuitant Indicator: 9 NOT APPLICABLE

29. Pay Rate Determinant: 0

30. Retirement Plan: KF [redacted]

31. Service Comp. Date (Leave): 01/20/2025

32. Work Schedule: F FULL TIME

33. Part-Time Hours Per Biweekly Pay Period:

POSITION DATA

34. Position Occupied: 3 (1 - Competitive Service; 2 - Excepted Service; 3 - SES General; 4 - SES Career Reserved)

35. FLSA Category: E (E - Exempt; N - Nonexempt)

36. Appropriation Code: 41AA0

37. Bargaining Unit Status: 8888

38. Duty Station Code: 11-0010-001

39. Duty Station (City - County - State or Overseas Location): WASHINGTON DISTRICT OF COLUMBIA DC

40. Agency Data	41.	42.	43.	44.
10001		0000	33.94	CRITICAL-SENSITIVE (CS)/HIGH R

45. Remarks

```
VETERAN PREFERENCE IS NOT APPLICABLE TO THE SENIOR EXECUTIVE SERVICE.
APPOINTMENT AFFIDAVIT EXECUTED 01-20-2025.
EMPLOYEE SUBJECT TO POST-EMPLOYMENT RESTRICTIONS UNDER 18 U.S.C. 207(C).
THE EMPLOYEE OCCUPIES A POSITION SUBJECT TO THE PAY FREEZE FOR CERTAIN SENIOR POLITICAL OFFICIALS.
 NOTWITHSTANDING OTHERWISE APPLICABLE PAY STATUTES AND REGULATIONS, PAY MAY BE SET AND ADJUSTED ONLY IN
 ACCORDANCE WITH APPLICABLE PROVISIONS OF THE PAY FREEZE STATUTE.
TENURE AS USED FOR 5 U.S.C. 3502 IS NOT APPLICABLE TO THE SENIOR EXECUTIVE SERVICE.
CREDITABLE MILITARY SERVICE: 0000
PREVIOUS RETIREMENT COVERAGE: NEVER COVERED
EMPLOYEE IS AUTOMATICALLY COVERED UNDER FERS, FERS-RAE, OR FERS-FRAE.
UPON APPOINTMENT TO THIS POSITION, APPOINTEE RECEIVED AND SIGNED THE ETHICS PLEDGE. MEMBER RECEIVED
 FINANCIAL DISCLOSURE MEMORANDUM AND SF-278 WHICH IS TO BE COMPLETED AND RETURN WITHIN 30 DAYS OF
 APPOINTMENT
```

46. Employing Department or Agency: OPM

47. Agency Code	48. Personnel Office ID	49. Approval Date
OM00	1000	01/27/2025

50. Signature/Authentication and Title of Approving Official
ELECTRONICALLY SIGNED BY:
CARMEN GARCIA-WHITESIDE
CHIEF HUMAN CAPITAL OFFICER AND DIRECTOR OF OPM HR

2 - OPF Copy - Long-Term Record - DO NOT DESTROY

Editions Prior to 7/91 Are Not Usable After 6/30/93
NSN 7540-01-333-6238

Standard Form 50
Rev. 7/91
U.S. Office of Personnel Management
FPM Supp. 296-33, Subch. 4

NOTIFICATION OF PERSONNEL ACTION

1. Name (Last, First, Middle) OPM-8	2. Social Security Number [redacted]	3. Date of Birth [redacted]	4. Effective Date 02/12/2025

FIRST ACTION

5-A. Code 570	5-B. Nature of Action CONV TO EXC APPT
5-C. Code Y7M	5-D. Legal Authority SCH C, 213.3391.
5-E. Code	5-F. Legal Authority

SECOND ACTION

6-A. Code	6-B. Nature of Action
6-C. Code	6-D. Legal Authority
6-E. Code	6-F. Legal Authority

7. FROM: Position Title and Number
SENIOR ADVISOR TO THE DIRECTOR
PD: 6A37370

8. Pay Plan	9. Occ. Code	10. Grade or Level	11. Step or Rate	12. Total Salary	13. Pay Basis
ES	0301	00	00	$195,200.00	PA

12A. Basic Pay	12B. Locality Adj.	12C. Adj. Basic Pay	12D. Other Pay
$195,200.00	$0	$195,200.00	$0

14. Name and Location of Position's Organization
OPM
OFC OF THE DIRECTOR
WASHINGTON DC

15. TO: Position Title and Number
SENIOR ADVISOR
PD: 6A39747

16. Pay Plan	17. Occ. Code	18. Grade or Level	19. Step or Rate	20. Total Salary/Award	21. Pay Basis
GS	0301	15	10	$195,200.00	PA

20A. Basic Pay	20B. Locality Adj.	20C. Adj. Basic Pay	20D. Other Pay
$162,672.00	$32,528.00	$195,200.00	$0

22. Name and Location of Position's Organization
OPM
OFC OF THE DIRECTOR
WASHINGTON DC

EMPLOYEE DATA

23. Veterans Preference: 1
1 - None; 2 - 5-Point; 3 - 10-Point/Disability; 4 - 10-Point/Compensable; 5 - 10-Point/Other; 6 - 10-Point/Compensable/30%

24. Tenure: 3
0 - None; 1 - Permanent; 2 - Conditional; 3 - Indefinite

25. Agency Use: JS

26. Veterans Preference for RIF: YES [✓ X] NO

27. FEGLI: B0 [redacted]

28. Annuitant Indicator: 9 NOT APPLICABLE

29. Pay Rate Determinant: 0

30. Retirement Plan: KF [redacted]

31. Service Comp. Date (Leave): 01/20/2025

32. Work Schedule: F FULL TIME

33. Part-Time Hours Per Biweekly Pay Period:

POSITION DATA

34. Position Occupied: 2
1 - Competitive Service; 2 - Excepted Service; 3 - SES General; 4 - SES Career Reserved

35. FLSA Category: E
E - Exempt; N - Nonexempt

36. Appropriation Code: 41AA0

37. Bargaining Unit Status: 8888

38. Duty Station Code: 11-0010-001

39. Duty Station (City - County - State or Overseas Location): WASHINGTON DISTRICT OF COLUMBIA DC

40. Agency Data	41.	42.	43.	44.
10001		0000	33.94	CRITICAL-SENSITIVE (CS)/HIGH R

45. Remarks
```
POSITION IS AT THE FULL PERFORMANCE LEVEL OR BAND.
OPM 1019 DATED 02-12-2025.
```

46. Employing Department or Agency: OPM

47. Agency Code	48. Personnel Office ID	49. Approval Date
OM00	1000	02/18/2025

50. Signature/Authentication and Title of Approving Official
ELECTRONICALLY SIGNED BY:
CARMEN GARCIA-WHITESIDE
CHIEF HUMAN CAPITAL OFFICER AND DIRECTOR OF OPM HR

APPOINTMENT AFFIDAVITS

Senior Advisor to the Director	01/20/2025
(Position to which Appointed)	(Date Appointed)

Office of Personnel Management	Office of the Director	Washington, DC, United States
(Department or Agency)	(Bureau or Division)	(Place of Employment)

I, OPM-8, do solemnly swear (or affirm) that--

A. OATH OF OFFICE

I will support and defend the Constitution of the United States against all enemies, foreign and domestic; that I will bear true faith and allegiance to the same; that I take this obligation freely, without any mental reservation or purpose of evasion; and that I will well and faithfully discharge the duties of the office on which I am about to enter. So help me God.

B. AFFIDAVIT AS TO STRIKING AGAINST THE FEDERAL GOVERNMENT

I am not participating in any strike against the Government of the United States or any agency thereof, and I will not so participate while an employee of the Government of the United States or any agency thereof.

C. AFFIDAVIT AS TO THE PURCHASE AND SALE OF OFFICE

I have not, nor has anyone acting in my behalf, given, transferred, promised or paid any consideration for or in expectation or hope of receiving assistance in securing this appointment.

OPM-8

(Signature of Appointee)

Subscribed and sworn (or affirmed) before me this 20 day of January, 2025

at Washington (City) DC (State)

[illegible]
(Signature of Officer)

(SEAL)

Commission expires ____________
(If by a Notary Public, the date of his/her Commission should be shown)

Acting Director
(Title)

Note - If the appointee objects to the form of the oath on religious grounds, certain modifications may be permitted pursuant to the Religious Freedom Restoration Act. Please contact your agency's legal counsel for advice.

Privacy Impact Assessment for

Government-Wide Email System (GWES)

February 28, 2025

Contact Point
Riccardo Biasini
Senior Advisor to the Director
Office of the Director

Reviewing Official
Greg Hogan
Chief Information Officer

OPM Form 5003

Legal Requirements for Privacy Impact Assessment

Longstanding Office of Management and Budget (OMB) and Office of Personnel Management (OPM) guidance explains that Privacy Impact Assessments (PIAs) are not required for IT systems or projects that collect, maintain, or disseminate information solely about federal government employees. For example, the OMB guidance states that "[n]o PIA is required . . . for government-run websites, IT systems or collections of information to the extent that they do not collect or maintain information in identifiable form about members of the general public." M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Attachment A(II)(B)(3) (Sept. 26, 2003); *see also id.* Attachment A(II)(B)(1) ("The E-Government Act requires agencies to conduct a PIA before: 1. developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public, or 2. initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government)."); OPM Privacy Impact Assessment (PIA) Guide, at 2 (Apr. 22, 2010) (stating that a PIA is required for "an IT system or project that collects, maintains, or disseminates information in identifiable form from or about members of the public"); *id.* at 3.

The Government-Wide Email System (GWES) collects, maintains, and disseminates information about federal government employees. Therefore, no PIA is required. OPM has nevertheless chosen to conduct this PIA in its discretion.

Abstract

OPM has a variety of personnel management functions, including executing, administering, and enforcing the civil service system. In order to carry out these duties, OPM internally developed the GWES to enable widespread,

rapid email communication with federal government employees. The GWES is designed to maintain the names and government email addresses of federal government employees, as well as emails sent from the system and responses to those emails.

Overview

To execute its authorized role with respect to personnel matters and fulfill its duty to enforce the civil service laws, OPM has developed a system to send government-wide emails to federal government employees and receive responses. This system increases efficiency and transparency by allowing fast and widespread communication with the federal workforce OPM has been tasked with overseeing.

The GWES system operates entirely on government computers and in Microsoft applications procured in the normal course. OPM uses this system to communicate with federal employees, in a capacity within its statutory authority. The GWES is designed to collect, maintain, and use the (1) names of federal employees, (2) their government email addresses, and (3) email messages and responses, which may include additional information about the employee provided by that employee. The GWES blocks responses from emails that do not have government domains.

The information in the GWES is accessible by a limited number of individuals within OPM who have a need for the information in the performance of their duties, overseen by the Chief Information Officer.

The GWES is built largely upon employee email contact information found in the Enterprise Human Resources Integration (EHRI) and Official Personnel Folder (OPF) record systems. Additional email contact data is collected from the employing agencies of federal workers. OPM applies filters to these various sources to remove erroneous domains before emails are sent. The GWES is subject to existing and approved OPM security plans and the data is stored in secure Microsoft applications and on government computers requiring PIV access.

Section 1.0. Authorities and Other Requirements

1.1. What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The President may delegate "authority for personnel management functions" to the Director of OPM. 5 U.S.C. § 1104(a)(1). OPM has been delegated authority to "exercise and provide leadership in personnel matters," among other functions. Executive Order 9830 § 01.2(b). The Director also has the duty to "execut[e], administer[], and enforce[e] … the civil service rules and regulations of the President and the Office and the laws governing the civil service." 5 U.S.C. § 1103(a)(5). Other relevant authorities include: 5 U.S.C. §§ 301, 2951, 3301, 4302, 6504, 8347, and 8461. These authorities permit OPM to maintain and request information regarding federal employees. The President may also, from time to time, direct OPM to collect information or communicate with the federal workforce on particular subject matters.

1.2. What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

Email systems are not generally subject to the Privacy Act of 1974. However, to the extent the GWES contain records subject to the Privacy Act, or information stored on secure government computers, the information in this system is covered by various OPM SORNs, including but not limited to OPM GOVT-1, GOVT-2, Central-21, and Internal-21 SORNs.

1.3. Has a system security plan been completed for the information system(s) supporting the project?

The GWES is located within Microsoft applications and on secure government computers. These Microsoft Applications have been granted an Authorization to Operate (ATO) that includes an approved system security plan. The government computers storing the data are subject to standard security requirements, including limited PIV access.

1.4. Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Depending on the nature and type of record within the GWES, various NARA-approved records schedules may apply. Item 040 (DAA-GRS-2017-0007-0004) covers any eOPF records and item 080 (DAA-GRS2017-0007-0012) covers other personnel contact information. Email records are governed by GRS 6.1, Capstone E-mail Retention.

1.5. If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Information contained in the GWES is not subject to the PRA because it is not collected from the public.

Section 2.0. Characterization of the Information

2.1. Identify the information the project collects, uses, disseminates, or maintains.

The GWES is designed to collect, maintain, and use the names and government email addresses of federal government employees. The GWES also maintains emails sent to those addresses, and collects and maintains responses to those emails. Specifically, the GWES contains the following:

- Employee Contact Data: The GWES is designed to collect, maintain, and use the names and government email addresses of federal government employees. Other identifying information is not used.

- Employee Response Data: After an email is sent using Employee Contact Data, the GWES stores that email and may collect and maintain responses. In some circumstances, responses may also be sent directly to or redistributed to employing agencies or other agencies consistent with applicable restrictions on the particular data at issue and using authorized means of transmission.

2.2. What are the sources of the information and how is the information collected for the project?

The Employee Contact Data is compiled using the EHRI and OPF record systems. Additionally, some email contact data is collected from the employing agencies of federal workers. The system applies filters to remove erroneous domains before emails are sent.

The Employee Response Data is sent by federal government employees to OPM by email.

2.3. Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No, although many names and email addresses of federal government employees are publicly available.

2.4. Discuss how accuracy of the data is ensured.

The Employee Contact Data comes from the EHRI and OPF systems, which are subject to their own accuracy measures as outlined in their respective PIAs, as well as directly from the employing agencies.

The Employee Response Data comes directly from employees through their secure government email addresses. OPM anticipates that the responses will cover information within employees' personal knowledge or information provided to them in the course of their official duties.

2.5. Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that erroneous email addresses have been collected.

Mitigation: This risk has been mitigated by compiling the Employee Contact Data through the EHRI and OPF systems, and directly from the employing agencies. The GWES uses email addresses with government domains and uses a filtering mechanism to remove contact data erroneously captured before emails are sent.

Privacy Risk: There is a risk that the Employee Response Data will be erroneous.

Mitigation: Because OPM uses the GWES to send emails to employees' official government email addresses, OPM has a high degree of confidence that the Employee Response Data will represent actual employee responses. Additionally, employees have the ability to correct any erroneous responses by working with the human capital officer or manager in their employing agency.

Section 3.0. Uses of the Information

3.1. Describe how and why the project uses the information.

The GWES enables OPM to communicate directly and quickly with federal government employees and help OPM fulfill its statutory and delegated duties to lead and oversee personnel management functions in the federal workforce. OPM may also further communicate employee responses to employing agencies to facilitate those agencies' own personnel management, or other agencies as appropriate to facilitate government-wide workforce initiatives.

3.2. Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how OPM plans to use such results.

OPM employees programmatically evaluate responses to verify the quality of the system and analyze the substance of the Employee Response Data. OPM anticipates enhancing and refining its response analyses over time. OPM may also query specific responses or emails to evaluate them as needed. Responses may be used to assist in making personnel decisions and to inform broader workplace initiatives.

3.3. Are there other programs or offices with assigned roles and responsibilities within the system?

No.

3.4. Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that the GWES information may be accessed by unauthorized users or by authorized users for an unauthorized purpose.

Mitigation: This risk is mitigated by restricting disclosure to a limited number of individuals who have a need to know the GWES information. The data is stored in secure Microsoft applications, and on secure government computers requiring a PIV card to access.

Section 4.0. Notice

4.1. How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

The names and government email addresses of federal government employees are already housed in OPM systems or provided by employing agencies and, in any event, do not contain substantive information about employees. As a result, there is no reason to provide advance notice for the collection of Employee Contact Data. Employees are provided notice of collection of the Employee Response Data in the emails disseminated using the GWES. Employees provide the data themselves in response to the email. This PIA also serves as a public resource explaining the purpose of the GWES, applicable SORNs, and other privacy-related information.

4.2. What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Individual federal government employees can decline to provide information by not responding to the email. The consequences for failure to provide the requested information will vary depending on the particular email at issue.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals will not know their information is being collected, maintained, and distributed through the GWES.

Mitigation: This risk is mitigated by the publication of this PIA and through various statements provided to government employees explaining the information collection at issue.

Section 5.0. Data Retention by the Project

5.1. Explain how long and for what reason the information is retained.

The records in the GWES are maintained according to the retention schedules identified in Section 1.4.

5.2. Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that the GWES information will be retained for longer than is necessary.

Mitigation: The risk is mitigated because OPM can delete all the GWES information, consistent with applicable retention schedules.

Section 6.0. Information Sharing

6.1. Is information shared outside of OPM as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

OPM anticipates regularly sharing GWES information relating to particular employees with their employing agency. In certain situations, data may also be shared with other agencies. Any data sharing will be undertaken consistent with applicable laws and policies, including pursuant to routine uses of applicable SORNs or employee consent. Data will be shared via authorized systems hosted either by OPM or the receiving agency.

6.2. Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

To the extent that GWES information is shared outside of OPM, it is shared consistent with applicable provisions of the Privacy Act, including through the routine uses of pertinent SORNs. The principal personnel SORN, GOVT-1, is owned by OPM but information may be accessed by employing agencies as needed.

6.3. Does the project place limitations on re-dissemination?

Government agencies that receive GWES information are generally subject to both the government-wide SORNs referenced in Section 1.2 as well as their own SORNs. Their use or disclosure of the information may occur only as consistent with applicable legal limitations.

6.4. Describe how the project maintains a record of any disclosures outside of OPM.

OPM keeps a record of distributions to the employing agencies in Microsoft applications. All actions taken by a user in Microsoft systems are logged, monitored, and accessed by those with a need to know for the performance of their official duties.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that GWES information will be shared outside of OPM without authorization.

Mitigation: This risk is mitigated by limiting access to the GWES and disseminating GWES information only as consistent with relevant SORNs or as otherwise permitted by applicable law.

Section 7.0. Redress

7.1. What are the procedures that allow individuals to access their information?

The federal government employees in the GWES have access to their own individual information. Employees will have a copy of any email that is sent, as well as their response. In addition, access procedures are outlined in each relevant SORN referenced in 1.2.

7.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

If the Employee Response Data is erroneous, any federal government employee covered by the GWES may inform the human capital officer or a manager in their employing agency, who can work with the employee and OPM as necessary to correct the problem.

7.3. How does the project notify individuals about the procedures for correcting their information?

Emails sent through the GWES, or related guidance disseminated through agency human capital officers or managers, may inform individual federal employees of the procedures for correcting erroneous information through their employing agency. Also, employees may follow the publicly accessible access and amendment procedures outlined in the relevant SORNs referenced in 1.2.

7.4. Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that federal government employees will not have information regarding how to amend erroneous information.

Mitigation: Lodging the primary corrective mechanism in the human capital officer or manager at the employing agency gives each employee intuitive and easy access to the corrective mechanism. Also, each SORN has clear access and amendment procedures that employees may follow.

Section 8.0. Auditing and Accountability

8.1. How does the project ensure that the information is used in accordance with stated practices in the PIA?

GWES information is captured by OPM's auditing tools and retained in an auditing archive. The Office of the Chief Information Security Officer reviews for suspicious or unusual activity and suspected violations, and appropriate action is taken as necessary.

8.2. Describe what privacy training is provided to users either generally or specifically relevant to the project.

OPM employees are required to take IT Security and Privacy Awareness training on an annual basis, and agree to OPM's Rules of Behavior before accessing the system.

8.3. What procedures are in place to determine which users may access the information and how does the project determine who has access?

Only a limited number of OPM employees with a need to know will have access to the full extent of the GWES data. No employee has access unless specifically authorized by the system owner and the authorizing official. Data sharing outside OPM is permitted only insofar as consistent with applicable law and as described above.

8.4. How does the project review and approve information sharing agreements, MOUs, new uses of the information, and new access to the system by organizations within OPM and outside?

Any changes in GWES access, uses, sharing agreements, or Memoranda of Understanding (MOUs) would need to be reviewed and approved by the system owner in coordination with the Office of the Chief Information Officer, as consistent with applicable law.

Responsible Officials

Office of the Chief Information Officer

Office of the Director

Approval Signature

Signed copy on file with the Chief Information Officer

Greg Hogan
Chief Information Officer

Introduction

Welcome to the Office of Personnel Management (OPM) Cybersecurity and Privacy Awareness Training

Welcome

This training course is designed to provide you with a basic understanding of your responsibilities in relation to the protection of OPM Information Systems and Information Resources.

OUR FIRST LINE OF DEFENSE - OUR EMPLOYEES

Cybersecurity and Privacy are the responsibility of every OPM employee, contractor, and other authorized users of OPM Information Technology and Information resources. Our technology and information are only as secure as the weakest link.

Training Requirements

This course is required for all OPM personnel (federal and contractor) who require access to OPM information systems and information resources.
At the end of this course there is a final quiz which will rate your understanding of the information provided.

What You Will Learn

Learn

You will **LEARN** about Cybersecurity and Privacy how it applies to you as a user of Information Systems and Information Resources.

Identify

You will be able to **IDENTIFY** Threats to OPM Information Systems and Information Resources.

Defend

You will be able to **DEFEND** against threats using defense mechanisms to protect Information Systems and Information Resources.

Acknowledgement of OPM Rules of Behavior

I understand that, when using OPM Information Systems and Information Resources, I am personally accountable for my actions and must comply with the OPM Rules of Behavior. The detailed OPM Rules of Behavior is provided in the Cybersecurity section of this course. An acknowledgement of the Rules of Behavior is provided in the Acknowledgement section of this course.

Lesson 1

CYBERSECURITY

WHAT IS CYBERSECURITY?

The National Institute of Standards and Technology (NIST) defines cybersecurity as *"Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation".*

CYBERSECURITY RISK

RISK - is a measure of the likelihood and the consequence of events or acts that could cause an information system compromise, including the unauthorized disclosure, destruction, removal, modification, or interruption of system assets or sensitive information resources.

THREAT - is any circumstance or event with the potential to harm an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. Threats arise from human actions, mechanical failures, and natural events, initiated by a threat source/actor.
VULNERABILITY - is a weakness in an information system, security procedures, internal controls, or implementation that could be exploited or triggered by a threat source/actor.
IMPACT - is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification/destruction/loss of information, or loss of information system availability.
Cybersecurity Risk is represented by the following formula:

RISK = THREAT x VULNERABILITY x IMPACT

CONFIDENTIALITY, INTEGRITY, AVAILABILITY (CIA)

A breach of security could adversely affect an OPM employee or OPM customers throughout the world. Therefore, everyone has a responsibility to protect the confidentiality, integrity, and availability of our information and systems. These terms, their objectives, and their loss potential are defined in the list below.

CONFIDENTIALITY

OBJECTIVE: To restrict information access and disclosure to those with the appropriate clearance and access level.
POTENTIAL FOR LOSS: The unauthorized disclosure of information.

INTEGRITY

OBJECTIVE: To ensure data entered and stored in information technology is correct.
POTENTIAL FOR LOSS: The unauthorized modification or destruction of information.

AVAILABILITY

OBJECTIVE: To ensure data and information is obtainable when needed.
POTENTIAL FOR LOSS: The disruption of access to information or an information system.

CYBERSECURITY LAWS AND POLICIES

As a user you will need to be aware of the Federal Laws and Agency Policies that govern the use of information systems and information.

LAWS

Various Federal policies and laws provide guidelines and regulations for securing information systems in the Government. Listed below are key laws and regulations significant to OPM information security.
The Federal Information Security Modernization Act of 2014 (FISMA)

Office of Management and Budget (OMB) Circular No. A-130, Managing Information as a Strategic Resource

POLICIES

There are a number of OPM Cybersecurity Policies that deal with the implementation of security measures and appropriate behaviors when utilizing OPM system and information resources. The core policies that effect you are as follows:

OPM Telework Policy
OPM Mobile Devices Policy
OPM Rules of Behavior
OPM Warning Banner
OPM Wireless Access Procedures
OPM Wireless Access Usage Restrictions

You may contact [redacted]@opm.gov for questions regarding Security Policies.

RULES OF BEHAVIOR

Upon being granted access to an OPM information system you will be required to acknowledge the following:

RULES OF BEHAVIOR FOR USERS OF INFORMATION TECHNOLOGY

As a user of OPM's computer systems, you are expected to understand and comply with OPM's Information Technology and Cybersecurity policies, and the responsibilities outlined below. Violations of these policies may result in the loss or limitation of access to OPM information and information systems, the initiation of administrative action consistent with current agency disciplinary procedures, and/or potential referral for appropriate criminal/civil proceedings. Every user is required to lock their system when leaving their workstation by removing their PIV card from the laptop or other computer device and completely exit the system at the end of the workday.

Protecting Personally Identifiable Information (PII) - You have the responsibility to protect PII whether you are working in an OPM facility or from home. This includes taking precautionary measures such as:

- Protecting your password;
- Do not leave materials containing PII out on your desk when not in immediate use;
- Do not walk away from your computer with a program or file open;
- Protect PII from others when in public spaces;
- Print PII and immediately retrieve it from the printer;
- Adhere to proper disposal measures, such as shredding;
- Encrypt emails containing PII when sending it outside OPM; and
- Only share PII with those who have a need to know in the course of their business;

Note: For more information on OPM's employee responsibilities for handling PII, email the Office of Privacy and Information Management at [redacted]@opm.gov.

Protection of Software, Data, and Hardware – You are not allowed to introduce any unauthorized software or data (including software and data protected by copyright, trademark, privacy laws, other proprietary data, or material with other intellectual property rights beyond fair use), hardware, or telecommunication devices or modify any configurations. You are not allowed to connect to other computer systems or networks without the authorization of OPM's Chief Information Security Officer.

Access to the OPM network must be authenticated with your PIV card. In addition, you will protect all sensitive information residing in OPM computer systems by preventing unauthorized access, use, modification, disclosure, or destruction of that information. This includes records about individuals requiring protection under the Privacy Act, sensitive information, trade secrets, intellectual property, and other information that is not intended for the public.

Service Restoration – You are responsible for assisting in restoring service in the event that the computer systems become non-operational. Priority is given to restoring the general support systems and the applications supporting OPM's mission-essential functions as defined in the agency's Continuity of Operations Plan.

System Privileges – You are given access to the computer systems based on a need to perform specific work at OPM. Users must not share their access rights with others. You are expected to work within the confines of the access allowed and are not to attempt to access systems or applications for which you are not authorized.

Telework – The OPM Human Resources Handbook, Chapter 368, Telework, contains the policy and procedures for authorizing telework. In general, immediate supervisors approve, on a case-by-case basis, employee requests to telework. Teleworkers who access OPM's general support systems must adhere to all IT security policy and procedures that would apply if the individual was accessing OPM's systems in the office.

Use of Government Office Equipment – You will comply with the policies specified in the OPM Policy on Personal Use of Government Office Equipment.

WARNING BANNER

Whenever you access an OPM information system you will be given a **WARNING BANNER** that expresses fundamental rules when accessing that information system. By utilizing that information system, you automatically accept these rules.

OPM WARNING BANNER

This is an Office of Personnel Management (OPM) computer system. OPM computer systems are to be used for official business and in accordance with the OPM Limited Personal Use Policy only.

You do not have the right to privacy while using any Government equipment including internet or email services. Furthermore, your use of Government office equipment for whatever purpose is not private or anonymous. While using Government office equipment your use may be monitored or recorded.

Unauthorized or inappropriate use of Government office equipment may result in the loss or limitation of your privileges.

You may also face administrative action ranging from counseling to removal from the Agency, as well as any criminal penalties or financial liability depending on the severity of the misuse.

OPM WIRELESS ACCESS USAGE RESTRICTIONS

Although OCIO provides tools and technologies to make the network and devices secure, OPM users have a responsibility to ensure that their wireless connection remains secure. Users must observe the following rules in order to ensure a safe and secure wireless connection:

All OPM-issued wireless devices to be used at OPM or for accessing OPM network and server resources will be purchased through the CIO as defined in the Information Technology Procurement Policy.

When desktop or laptop computers are connected physically to the OPM network via a network cable, wireless will be disabled automatically.

For those traveling with mobile devices to locations outside the United States, they must take extra measures to physically safeguard those devices. Check the U.S. State Department Current Travel Advisories for specific country information.

Upon return from locations with "current travel warnings" users must return mobile devices to OPM Customer Support (Help Desk) for inspection and/or re-imaging as appropriate. The use of Bluetooth or infrared technologies is currently prohibited on OPM's network. Desktop or laptop computers will be configured in a manner that disables these features.

Users can connect to OPM through cellular technology (using an air card, for example) or through a Wi-Fi connection but not both at the same time.

In an effort to ensure the highest level of security while accessing network and server resources, devices connected to OPM network and server resources may be disconnected if they are not configured properly.

OPM users need to ensure that their physical environment is protected from unauthorized viewing of login credentials and OPM data.

OPM users need to report any incident or suspected incidents or unauthorized access and/or disclosure of OPM's information and technology resources to their manager and OPM's Security Monitoring Center at [redacted]***@opm.gov*** or 844-[redacted].

OPM WIRELESS ACCESS PROCEDURES

These procedures describe the actions necessary to comply with OPM's security control requirements for wireless access:

Wireless Access Monitoring - OPM checks for unauthorized wireless access to the Local and Wide Area Network (LAN/WAN) by monitoring all Virtual Private Network (VPN) traffic from remote devices. Suspicious activities from VPN connections are investigated to validate risks and perform remedial actions as necessary.

Two-Factor Authentication - OPM authorizes wireless access via two-factor authentication to OPM's VPN. All external OPM wireless access is technically forced to authenticate to OPM's VPN prior to establishing connectivity to the network.

Access Control Enforcement - Enforcement of OPM's wireless access controls is technically accomplished with FIPS 140-2 approved VPN authentication. Enforcement is also implemented through continuous monitoring and ongoing assessments of existing planned controls.

RIGHT TO PRIVACY

Activity on Government computers is monitored for security reasons. When you log on to a government system, you give your consent to this monitoring; therefore, the right to privacy does not apply to your computer use. Also, keep in mind that the following activities or Websites are prohibited on Government computers:

- **Adult Content**
- **Gambling**
- **Private Business Activities**
- **Unauthorized Configuration Changes**
- **Online Auctioning**

.GOV EMAIL ACCOUNT

Your OPM email address is only for **OFFICIAL** government activities and not used for personal use on any website. This will reduce the potential for compromise. If you have used your .gov email address, change your account information to an alternate/personal email account.

Lesson 2

PRIVACY

What You Will Learn

After completing this training module, you will:

- Understand what Personally Identifiable Information (PII) is
- Understand your responsibility to safely handle PII
- Know how to recognize and respond to a breach of PII
- Know your obligations under the Privacy Act and the e-Government Act

PERSONALLY IDENTIFIABLE INFORMATION (PII)

PERSONALLY IDENTIFIABLE INFORMATION (PII) is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Common examples of PII include:

- Name (name by itself is PII)
- Social Security number (SSN)
- Date of birth (DOB)
- Mother's maiden name
- Financial records, including bank account or other financial account numbers (Credit card information)
- Address (both physical and email)
- Retirement account number
- Health information
- Business contact information (Phone number)
- Driver’s license number
- Passport number
- Race and Ethnicity
- Sex
- Gender
- Disability
- Biometric Identifiers

Because there are many types of information that can be used to distinguish or trace an individual's identity, this definition is necessarily broad – and not limited to the above list.

Information that on its face does not appear to be PII can become PII if it is linked, or linkable, to another piece of information about a particular individual. For example, yellow shirt or brown hair when used to distinguish one person from another are PII, whereas standing alone and not linked or linkable to an individual they are not.

SENSITIVE PII

The loss or compromise of some PII can cause harm to an individual – to include financial harm, embarrassment, or unfairness. The sensitivity of PII must be evaluated in context to determine the risk of harm to an individual in the event of a loss or compromise. For example, a list of names in a public directory may not be sensitive, but a list of names of individuals who received poor performance reviews is.
Certain information standing alone is sensitive and creates risk to an individual. For example, personal financial account numbers, drivers' license or state ID numbers, and biometric identifiers, alone, are sensitive PII. Social Security numbers (SSNs) are also a common example of sensitive PII. Other PII is sensitive in combination: For example, a date of birth combined with an individual's name is sensitive PII, whereas standing alone and not linked or linkable to another identifying data element it is not.

HANDLING PII

Protecting PII is everyone's responsibility. Be aware of what PII you have in your possession and the PII that resides in any electronic system you access. Be vigilant when handling PII so that it is not lost or compromised. To that end:

- Limit your access to only the PII that you have a need to know and do not disclose or provide access to others unless they also have a need to know for a legitimate business purpose.
- Do not leave documents containing PII visible or unattended on your desk. At the end of the day, either secure them in a locked office or in a locked drawer. Lock your computer and remove your PIV card when leaving your laptop, even for a brief time.

HANDLING PII - Email

- When sending PII over email or responding to an email containing PII, double check email addresses to make sure you have selected the correct recipients and double-check your attachment to make sure you have selected the correct document. Ask yourself: is there any PII in the message? Where is the PII located in the message? Where are you sending the email? Never include a SSN or PII as a reference number on tracking forms, return receipts or envelopes or packages.

- When emailing PII, be aware that the autofill function may populate the wrong recipient, and you should take care to check that you are sending the email only to those who have a need to know the information for a legitimate business need. If you are sending to multiple people or a distribution list, make sure what you are sending is appropriate for every recipient.

- Only send sensitive PII via email using "Send Secure" or other means approved by the Chief Information Security Officer. Sensitive email sent internally within OPM does not require additional encryption however, users should share files via OCIO approved technologies such as OneDrive, Teams, or SharePoint rather than including sensitive attachments. In either case, consider the business need and check your message carefully before sending PII to either external or internal parties.

HANDLING PII - Printers and Fax Machines

- Do not leave documents containing PII unattended at a printer. If you are printing PII to a shared printer, verify the location of the printer prior to sending the document to print and immediately retrieve the printed material.

- Likewise, when you send PII via Fax machine, doublecheck fax numbers before dialing, and before transmitting and call the recipient BEFORE and AFTER the transmission for verification it was received by the right person.

HANDLING PII - Oral Communication

- Do not discuss PII in public places, such as restaurants, elevators, hallways, bathroom, or outside OPM, where others without a need to know may hear the discussion.

HANDLING PII - Mail

- Dispose of documents containing PII appropriately, such as by shredding or placing in a locked bin or burn bag. Do not place them in a trash can or general recycling bin.
- When mailing PII, make sure that only information intended for the recipient to whom the mail is addressed is included in the envelope. Do not mark the envelope in any way that would call attention to the fact the sensitive information is enclosed. If possible, all such mailings should be sent in a manner that can be tracked, such as return receipt requested, so that you are certain it has reached its intended recipient.

HANDLING PII - Teleworking

There are additional considerations in place for protecting PII in telework locations.

Program offices may have their own respective policies in place for transporting PII. Generally, moving PII from your OPM location to home and back requires supervisory approval. You should provide your supervisor with a list of all printed documents to be moved to ensure accountability of documents. PII should be physically secured while in transit. Documents should not be left in plain sight or unattended in a private vehicle or other modes of transportation.

While teleworking, either in a maximum telework or routine telework situation, please be extra careful of leaving PII exposed that others in your household may inadvertently see and make sure the PII materials are disposed of properly. Only use OPM-approved portable electronic devices and password-protect all documents containing PII. You should secure all notes, documents, and portable media devices when not in use. Make sure that you keep your work files separate from personal files. Do not forward work emails to your personal or web-based email accounts. Do not take personnel-related data home without permission of your supervisor. Do not leave personnel-related data unattended at home.

Only government-furnished printers (designated by OPM's OCIO) may be used at an alternative site. Do not print OPM documents on a personal home printer. Government-furnished printers may be used only by OPM employees, and not by family members. If employees have been approved to print documents at home, they must maintain a controlled environment for printed documents, such as a locking cabinet or locked office. Other individuals, including family members, should not have access to printed documents.

Employees should dispose of all printed materials (including drafts, and PII) appropriately using a cross-cutting shredder. Program offices may purchase shredders approved for purchase by CIO. If your office does not purchase a shredder for an alternative site, you are still responsible for shredding documents privately, or securely transporting materials to OPM and use the office shredder or place in OPM's protected bins.

Make sure that any shared network folder where you store PII is accessible only to those who have a need to know the information for a legitimate business purpose.

As a reminder, regardless of where printed records are kept at the office or in a telework environment, they are part of the OPM records system and are subject to the requirements of the OPM records management program.

Vulnerable Areas Where PII Can Be Compromised - Trash

- Dispose of unwanted documents or disks containing sensitive data appropriately. Use the burn bags and locked trash bins for sensitive material.
- Use caution when discarding information in your waste bin. Once trash leaves the office, we lose control over it, and it can become vulnerable. Think about what someone could find out about you or your work if they examined documents in your waste bin!
- Sensitive documents must be shredded or placed in an area where the paper will be picked up and shredded later.

Vulnerable Areas Where PII Can Be Compromised - Fax Machines and Printers

- Double check fax numbers before dialing, and before transmitting, to ensure you have the correct number.
- Call the recipient BEFORE and AFTER the transmission for verification it was received by the right person.

- Verify your printer location PRIOR to sending a document to the printer.
- Promptly pick up ALL copies of the documents.
- Dispose of sensitive documents appropriately, e.g., shred them.
- Use a special trash receptacle for sensitive papers or a paper shredder.

BREACHES OF PII

Sometimes, regardless of how careful you are in handling PII, it may be lost or compromised. This is a "breach," defined as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for an other than authorized purpose. OMB Memorandum M-17-12, Preparing for and Responding to Breach of Personally Identifiable Information.

A breach is not limited to an occurrence where a person other than an authorized user potentially accesses PII electronically, by, for example, a network intrusion, a targeted attack exploiting website vulnerabilities, or an attack executed through an email message or attachment.

A breach may also include the loss or theft of physical documents that include PII and portable electronic storage media that store PII, the inadvertent disclosure of PII on a public website, an oral disclosure of PII to a person who is not authorized to receive that information, or inadvertently sending an email containing PII to a recipient who does not have a business need to receive the information.

COMMON BREACH SCENARIOS

The following are some common breach scenarios:

- A laptop or portable storage device storing PII is lost or stolen.
- An email containing PII is inadvertently sent to the wrong party.
- A box of documents containing PII is lost or stolen during shipping.
- An unauthorized third party overhears agency employees discussing PII about an individual seeking employment or Federal benefits.

- A user with authorized access to PII uses it for personal gain or disseminates it to embarrass an individual.
- An IT system that maintains PII is accessed by a malicious actor.
- Mail enclosing PII sent out from OPM is either not sealed or PII information is visible when the letter is enclosed in a window envelope.
- PII that should not be widely disseminated is posted inadvertently on a public website.

REPORTING A BREACH

IMMEDIATELY report ANY breach by emailing [redacted]@opm.gov or by calling 844[redacted]. Also, notify your supervisor. Report all losses or potential losses of PII, regardless of whether you think it is sensitive or not.

Reporting a breach is necessary so that appropriate steps can be taken to mitigate the breach and minimize the risk to the individuals whose PII may have been compromised. All breach reports submitted to CyberSolutions are reviewed by Office of Executive Secretariat and Privacy and Information Management staff.

Social Security Number Justification

Authorities

- OMB Circular No. A-130, Managing Information as a Strategic Resource

Policy

- All OPM personnel shall reduce or eliminate the use of SSNs wherever possible
- Use of the SSN includes the SSN in any form, including, but not limited to, truncated, masked, partially masked, encrypted, or disguised SSNs
- SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria
- SSNs shall be used in approved forms and systems when they meet one or more of the acceptable use criteria
- Specific reviews of forms and systems shall be conducted to reduce SSN use

FAIR INFORMATION PRACTICE PRINCIPLES (FIPPs)

The Fair Information Practice Principles (FIPPs) are a collection of widely accepted principles that provide a consistent framework for analyzing, evaluating, and developing policy concerning our collection, maintenance, use, and dissemination of personally identifiable information (PII) and the effect on individual privacy. As articulated most recently in the Office of Management and Budget Circular A-130, the FIPPs are:

Access and Amendment: provide individuals with appropriate access to and ability to correct their information.

Accountability: be accountable for and document compliance with applicable privacy requirements.

Authority: collect, maintain, and use PII only if you have the authority to do so.

Minimization: collect, maintain, and use only PII that is directly relevant and necessary to accomplish a legally authorized purpose.

Quality and Integrity: collect, maintain, and use PII that is as accurate, relevant, timely, and complete as is reasonably necessary to ensure fairness to the individual.

Individual Participation: involve the individual in the process of using their PII and seek consent where practicable.

Purpose Specification and Use: provide notice of the specific purpose for which PII is collected and only use, maintain, or disclose it for that purpose.

Security: establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use and destruction.

Transparency: be transparent and provide notice about information policies and practices concerning PII.

To learn more about the FIPPs, please watch this Federal Privacy Council video.

THE PRIVACY ACT

The Privacy Act is the cornerstone of federal privacy law and provides rights and protections for individuals whose information the Executive Branch requires to carry out its mission of serving the American people. The Act balances the government's need to maintain information about individuals with the rights of those individuals to be protected from unwarranted invasions of their privacy. It does this by:

- Restricting the disclosure of individuals' information.
- Providing access and amendment rights to individuals whose information has been collected; and
- Establishing a set of fair information practice principles regarding the collection, maintenance, use, and dissemination of individuals' information.

More specifically, the Privacy Act applies to records about U.S. citizens and lawful permanent residents contained in an agency "system of records." A "system of records" is a group of records from which information is retrieved by a name or other identifier. For every system of records, an agency must publish a system of records notice, or SORN, in the Federal Register. A list of OPM's SORNS can be found at https://www.opm.gov/privacy.

To learn more about the Privacy Act of 1974, please watch this Federal Privacy Council video.

THE E-GOVERNMENT ACT and PRIVACY IMPACT ASSESSMENTS

The E-Government Act requires you to conduct a Privacy Impact Assessment (PIA) whenever you develop, procure, or use information technology to create, collect, store, process, maintain, disseminate, or dispose of personally identifiable information (PII). The assessments are documented and presented to the public on OPM's website, and these documents provide transparency to the public about OPM's collection, use, and dissemination of PII.

A PIA explains what information is being collected, how OPM intends to use that information, who it will be shared with, how it is secured, and whether individuals can approve or decline the use of their information. The PIA employs the FIPPs to identify and evaluate privacy risk by, for example, examining whether only the minimum information needed to achieve the intended purpose is collected and whether mechanisms are in place to reasonably ensure accuracy.

OPM's PIAs are available at https://www.opm.gov/privacy.

To learn more about Privacy Impact Assessments, please watch this Federal Privacy Council video.

Lesson 3

THREATS

WHAT IS A CYBERSECURITY THREAT?

NIST defines a Threat as, *"Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service."*

THREAT SOURCES

The following is a listing of potential Threat Sources:

HUMAN - ADVERSARIAL

Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).

- **INDIVIDUAL** (Outsider, Insider, Trusted Insider, Privileged Insider)
- **GROUP** (Ad Hoc, Established)
- **ORGANIZATION** (Competitor, Supplier, Partner, Customer)
- **NATION STATE** (Foreign Nation)

HUMAN - ACCIDENTAL

Erroneous actions taken by individuals in the course of executing their everyday responsibilities.

- **USER** (General users of an information system)

- **PRIVILEGED USER/ADMINISTRATOR** (Users with advanced system permissions)

STRUCTURAL

Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.

- **IT EQUIPMENT** (Storage, Processing, Communications, Display, Sensor, Controller)
- **ENVIRONMENTAL CONTROLS** (Temperature/Humidity, Power Supply)
- **SOFTWARE** (Operating System, Networking, General-Purpose Application, Mission-Specific Application)

ENVIRONMENTAL

Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization.

- **NATURAL OR MAN-MADE DISASTER** (Fire, Flood, Tornado, Hurricane, Earthquake, Bombing, Overrun)
- **UNUSUAL NATURAL EVENT** (Sunspots, Meteor Shower)
- **INFRASTRUCTURE FAILURE/OUTAGE** (Telecommunications, Power Grid)

THREAT ATTACK METHODS

There are many attack methods utilized by Threat Actors. Here are the most common encountered.

SOCIAL ENGINEERING

Social Engineering is an attack vector used to gain access to networks, systems, or physical locations, or for financial gain by using human psychology, rather than using technical hacking methods. It relies on social interaction to manipulate people into circumventing security best practices and protocols.

Social engineering is the new preferred tactic among the hacker community. It is easier to exploit users' flaws than to discover a vulnerability in networks or systems.

Social Engineering is based on taking advantage of the following:

Heightened Human Emotions - Emotional manipulation gives attackers the upper hand in an interaction. You are far more likely to take irrational or risky actions when in an enhanced emotional state. The following emotions are all used in equal measure to convince you.

These emotions include: Fear, Excitement, Curiosity, Anger, Guilt, and Sadness.

Urgency - Time-sensitive opportunities or requests are another reliable tool in an attacker's arsenal. You may be motivated to compromise yourself under the guise of a serious problem that needs immediate attention. Alternatively, you may be exposed to a prize or reward that may disappear if you do not act quickly. Either approach overrides your critical thinking ability.

Trust - Believability is invaluable and essential to a social engineering attack. Since the attacker is ultimately lying to you, confidence plays an important role here. They've done enough research on you to craft a narrative that's easy to believe and unlikely to rouse suspicion.

MALICIOUS CODE

Malicious code is the term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system. Malicious code describes a broad category of system security terms that includes attack scripts, viruses, worms, Trojan horses, backdoors, and malicious active content.

HACKING

Hacking is the process of gaining unauthorized access to a computer network or an electronic device. Individuals breach into a system either to cause harm or to highlight vulnerabilities in existing security measures.

There are some others whose motives remain ambiguous or even double-sided. Hackers are of six main types:

WHITE HAT HACKER - White hat hackers are the ethical hackers who use their skills to discover loopholes in existing cybersecurity measures to help fix them.

BLACK HAT HACKER - Black hat hackers are malicious individuals in cyberspace who try and break into systems & networks to steal confidential information. In addition to stealing, a black hat hacker may also delete or modify certain crucial files to cause disruption and inflict losses.

GRAY HAT HACKERS - Grey hat hackers use methods that are similar to those of white and black hat hackers. However, they do not have any malicious intentions. A gray hat hacker may breach into a company's private servers, but instead of stealing information, will notify management about the vulnerability.

RED HAT HACKER - Red hat hackers are similar to policing agents on the internet. They actively search for black hat hackers and shut them down. Whenever they find one, they don't report the hacker to the authorities, but take matters into their own hands. A red hat hacker will hack the would-be attackers' computer and halt their malicious activities.

BLUE HAT HACKER - A blue hat hacker can be malicious but usually, that anger is channeled at one person or company. They seek revenge for some type of wrong. Blue hats are typically new to hacking and may start out as Script Kiddies. An event or incident may turn them from being nonchalant about hacking to being focused on exacting some kind of hacking catastrophe for their target.

GREEN HAT HACKER - Green hat hackers are newbies, and they are working to improve their skills every day so they can become better. The green hat has something to prove and often gets chided by the hacking community if they ask basic questions. Yet, their desire to learn keeps them asking. They may idolize well-known black hats and are desperate to elevate themselves to the real world of hacking.

HACKTIVISTS - Hacktivists break into government or corporate systems out of protest. They use their skills to promote a political or social agenda. Targets are usually government agencies or big corporations.

SCRIPT KIDDIES - Script kiddies are hackers who are new to hacking and don't have much knowledge or skills to perform hacks. Instead, they use tools and scripts developed by more experienced hackers.

DENIAL OF SERVICE

A Denial-of-Service (DoS) is any type of attack where the attackers attempt to prevent legitimate users from accessing the service. In a DoS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses. The network or server will not be able to find the return address of the attacker when sending the authentication approval, causing the server to wait before closing the connection. When the server closes the connection, the attacker sends more authentication messages with invalid return addresses. Hence, the process of authentication and server wait will begin again, keeping the network or server busy.

DISTRIBUTED DENIAL OF SERVICE

A Distributed Denial-of-Service (DDos) is a consorted event where multiple attackers or entities coordinate a DoS attack on a specific resource.

Clickjacking

Clickjacking - Clickjacking, also known as a "UI redress attack", is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top-level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to another page, most likely owned by another application, domain, or both. (OWASP.org).

THREAT - SOCIAL ENGINEERING

This attack vector relies on social interaction to manipulate people into circumventing security best practices and protocols.

PHISHING

Phishing is the most common type of social engineering attack that occurs today. Most phishing scams endeavor to accomplish three things:

- Obtain personal information such as names, addresses and Social Security Numbers.
- Use shortened or misleading links that redirect users to suspicious websites that host phishing landing pages.
- Incorporate threats, fear, and a sense of urgency in an attempt to manipulate the user into responding quickly.

DECEPTIVE PHISHING

Deceptive phishing is by far the most common type of phishing scam. In this ploy, fraudsters impersonate a legitimate company in an attempt to steal people's personal data or login credentials. Those emails frequently use threats and a sense of urgency to scare users into doing what the attackers want.

SPEAR PHISHING

Not all phishing scams embrace "spray and pray" techniques. Some ruses rely more on a personal touch. They do so because they wouldn't be successful otherwise.

In this type of ploy, fraudsters customize their attack emails with the target's name, position, company, work phone number and other information in an attempt to trick the recipient into believing that they have a connection with the sender. Yet the goal is the same as deceptive phishing.

Given the amount of information needed to craft a convincing attack attempt, it's no surprise that spear-phishing is commonplace on social media sites like LinkedIn where attackers can use multiple data sources to craft a targeted attack email.

WHALING

Spear phishers can target anyone in an organization, even executives. That's the logic behind a "whaling" attack. In these scams, fraudsters try to harpoon an exec and steal their login details.

VISHING

This type of phishing attack dispenses with sending out an email and instead goes for placing a phone call. An attacker can perpetrate a vishing campaign by setting up a Voice over Internet Protocol (VoIP) server to mimic various entities in order to steal sensitive data and/or funds.

SMISHING

This method leverages malicious text messages to phones to trick users into clicking on a malicious link or handing over personal information.

PHARMING

As users become wiser to traditional phishing scams, some fraudsters are abandoning the idea of "baiting" their victims entirely. Instead, they are resorting to pharming. This method of phishing leverages cache poisoning against the domain name system (DNS), a naming system which the Internet uses to convert alphabetical website names, such as "www.microsoft.com," to numerical IP addresses so that it can locate and thereby direct visitors to computer services and devices.

PRETEXTING

Pretexting is another form of social engineering where attackers focus on creating a good pretext, or a fabricated scenario, that they use to try and steal their victims' personal information. In these types of attacks, the scammer usually says they need certain bits of information from their target to confirm their identity. In actuality, they steal that data and use it to commit identity theft or stage secondary attacks.

More advanced attacks sometimes try to trick their targets into doing something that abuses an organization's digital and/or physical weaknesses. For example, an attacker might impersonate an external IT services auditor so that they can talk a target company's physical security team into letting them into the building.

Whereas phishing attacks mainly use fear and urgency to their advantage, pretexting attacks rely on building a false sense of trust with the victim. This requires the attacker to build a credible story that leaves little room for doubt on the part of their target.

Pretexting can and does take on various forms. Even so, many threat actors who embrace this attack type decide to masquerade as HR personnel or employees in the finance department.

BAITING

Baiting is in many ways similar to phishing attacks. However, what distinguishes them from other types of social engineering is the promise of an item or good that malicious actors use to entice victims. Baiters may leverage the offer of free music or movie downloads, for example, to trick users into handing over their login credentials.

Baiting attacks are not restricted to online schemes. Attackers can also focus on exploiting human curiosity via the use of physical media.

QUID PRO QUO

Similar to baiting, quid pro quo attacks promise a benefit in exchange for information. This benefit usually assumes the form of a service, whereas baiting usually takes the form of a good.

Popular baiting comes from actors pretending to be from employees of the Social Security Administration (SSA) or Internal Revenue Service (IRS).

CLICKJACKING

Clickjacking, also known as a “UI redress attack”, is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top-level page. Thus, the attacker is “hijacking” clicks meant for their page and routing them to another page, most likely owned by another application, domain, or both. (OWASP.org).

PHYSICAL

Some Social Engineering relies on the physical presence of the threat actor to perpetrate.

TAILGATING

In these types of attacks, someone without the proper authentication follows an authenticated employee into a restricted area. The attacker might impersonate a delivery driver and wait outside a building to get things started. When an employee gains security’s approval and opens the door, the attacker asks the employee to hold the door, thereby gaining access to the building.

Tailgating, also known as "piggy backing", does not work in all corporate settings such as large companies whose entrances require the use of a keycard. However, in mid-size enterprises, attackers can strike up conversations with employees and use this show of familiarity to get past the front desk.

SHOULDER SURFING

In this type of attack someone can sneak up next to or behind a person to view the information on the computer screen of a user without their knowledge.

EAVESDROPPING

In this type of attack someone lurking nearby can listen in on person-to-person conversation (as well as phone conversation) when individuals are discussing sensitive information that could be used in other Social Engineering endeavors.

BORROWING

In this type of attack someone may ask to use your phone or computer to access a site or lookup their email because theirs is not working, or they forgot it at home. This will give them access to your personal resources and access privileges.

THREAT - MALICIOUS CODE 1

This attack vector relies on installation of computer code (software or firmware) that circumvent implemented security programs and protocols.

VIRUSES

A virus is a malicious program that modifies other host files or boot areas to replicate. In most cases the host object is modified to include a complete copy of the malicious code program. The subsequent running of the infected host file or boot area then infects other objects.

WORMS

A worm is a sophisticated piece of replicating code that uses its own program coding to spread, with minimal user intervention. Worms typically use widely available applications (e.g., email, chat channels) to spread. A worm might attach itself to a piece of outgoing email or use a file transfer command between trusted systems. Worms take advantage of holes in software and exploit systems. Unlike viruses, worms rarely host themselves within a legitimate file or boot area.

TROJAN HORSES

A Trojan, or Trojan horse, is a nonreplicating program masquerading as one type of program with its real intent hidden from the user. For example, a user downloads and runs a new, free version of his favorite multiplayer game from a web site. The game promises thrills and excitement. But its true intent is to install a Trojan routine that allows malicious hackers to take control of the user's machine. A Trojan does not modify and infect other files.

THREAT - MALICIOUS CODE 2

This attack vector relies on installation of computer code (software or firmware) that circumvent implemented security programs and protocols.

KEYLOGGER

A specific type of spyware is known as a keylogger (or a “keystroke logger” for you more specific readers). A keylogger is a type of hardware or software that records everything you type without needing access to what’s on your monitor. That’s because it records all of your keyboard activities — basically, every keystroke you type on your keyboard. The benefit of this to hackers is that it allows them to monitor your activities and capture sensitive information such as your account credentials and passwords.

ROOTKITS

A rootkit is a remote access tool (RAT) or application that provides remote admin access to devices. This isn’t bad in and of itself. But, as you can imagine, this means that they can cause a lot of damage if they’re put to work by someone with devious intentions.

BOTS AND BOTNETS

A botnet is a network of compromised computers, servers, and Internet of Things (IoT) devices (infected devices that are also sometimes called bots or zombies). The devices are infected with a malware and form a massive weapon that cybercriminals can use to launch massive, distributed denial of service (DDoS) attacks against individuals, governments, and organizations. These attacks inundate the target with traffic requests or packets to disrupt the server or network, or to take it offline completely.

THREAT - MALICIOUS CODE 3

This attack vector relies on installation of computer code (software or firmware) that circumvent implemented security programs and protocols.

ADWARE

Adware is not in itself malware but is an embedded portion of software that periodically pushes ads inside the application running or as popups. In some instances, Adware can sometimes assist in the delivery of other malware, which may often include spyware. Adware can just as easily be harmless and respectful, whereas others might be invasive and irritating.

SCAREWARE

Scareware is a malware tactic that manipulates users into believing they need to download or buy malicious, sometimes useless, software. Most often initiated using a pop-up ad, scareware uses social engineering to take advantage of a user's fear, coaxing them into installing fake anti-virus software.

RANSOMWARE

Ransomware is a type of malware that encrypts a target's data until some demand is satisfied — typically, the payment of a ransom. (Hence the clever malware name.)

THREAT - INSIDER

An insider is anyone given approved access to an agency's system and information (data) resources and through an action/activity initiated by them and causes harm to the agency's system and/or information resources. Their approved access can be current or expired. Insiders can include current or former employees, contractors, or business partners.

MALICIOUS INSIDER

A Malicious Insider is one who maliciously and intentionally abuses legitimate credentials, typically to steal information for financial or personal incentives. Malicious Insiders have an advantage over other attackers because they are familiar with the security policies and procedures of an organization, as well as its vulnerabilities.

Other forms of the Malicious Insider are:

- **Professional Insider** - An Insider with the knowledge and intent to circumvent security policies and procedures to exploit the agency's system and information resources. This includes the printing and copying of sensitive information (e.g. PII, and Financial Information).
- **Insider Agent** - A person working with another Threat Source (Insider or Hacker) to provide access to resources or information to exploit weaknesses.

NEGLIGENT INSIDER

A Negligent Insider is one who intentionally or unintentionally through their inaction/inactivity causes the exploit of the agency's system and information resources or abuses legitimate credentials, typically to steal information for financial or personal incentives. Malicious Insiders have an advantage over other attackers because they are familiar with the security policies and procedures of an organization, as well as its vulnerabilities.

ACCIDENTAL INSIDER

An Accidental Insider is one who, through action or inaction without malicious intent, causes harm or substantially increases the probability of future serious harm to an organization’s information or information systems. The Accidental Insider usually performs an action or activity contrary to organizational security guidance or security best practices.

THREAT - INSIDER - EXAMPLE

Difference between a Malicious and Accidental Insider Threat

MALICIOUS

The disgruntled employee was upset over not being promoted to a new position and wanted to get even with management.

The User has access to system resources and bad intent to cause harm to the agency's system and information resources.

ACCIDENTAL

A new unsupervised employee deletes the wrong customer account.

The User has access to system resources but does not have bad intent to cause harm to the agency's system and information resources.

CYBER ALERT RELATED TO WORLD EVENTS

CYBER ALERT RELATED TO WORLD EVENTS

Many world events are on the minds of individuals around the globe. Unfortunately, cyber-attackers are likely to use the public's interest and concern to their advantage. History has shown that cybercriminals monitor current events closely, quickly developing and distributing malicious content, including:

• Phishing emails, text messages, and phone calls

• Fraudulent online ads and social media posts

• Lookalike websites

You might encounter threats in the form of:

• Sensationalized stories that seem to come from legitimate news outlets

• Inflammatory claims and other forms of misinformation

• Fake charity and assistance organizations

Those who engage with fraudulent content could reveal sensitive personal data or expose themselves (and our organization) to malicious software (malware).

You must remain alert to attackers' attempts to manipulate you and trick you into taking a dangerous action. Apply what you've learned in your security awareness training to ensure you're making the best choices. Be sure to report ANY suspicious emails by clicking the "Report Phishing" button in Outlook.

Lesson 4

CYBER-DEFENSE

LINES OF CYBER-DEFENSE

Like a castle defending against a siege, OPM has several layered security defenses to protect its information systems, data, and personnel from threat actors.

DATA LAYER - is where all OPM's information resides. At this layer the data is protected when at rest (stored) and while in transport (being processed by an application or transmitted across the network).

APPLICATION LAYER - is where data is processed and accessed by users. This layer uses protection mechanisms that promote "**Least Privilege**" (the principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function) and "**Separation of Duties**" (also known as "Keys to the Kingdom", this refers to the principle that no user should be given enough privileges to misuse the system on their own).

ENDPOINT LAYER - is where applications reside, operate, and connect to networked resources. Hardware devices that reside on the agency's network (.e.g Computers, Phones, Printers, etc.) where applications reside and operate.

NETWORK LAYER - is the hardware and software infrastructure that connects all endpoints together and manages the communications between those devices as well as external through the perimeter.

PERIMETER LAYER - is the hardware and software infrastructure that connects the internal OPM network externally (outside OPM). This layer manages all communications between internal and external information resources.

PHYSICAL LAYER - is the physical infrastructure that protect the agency's information assets to include the building, data center, equipment racks, storage cabinets.

POLICY LAYER - this layer provides the rules for development and implementation of the agency's cyber-defense layers to protect agency information assets.

HUMAN LAYER - OPM Federal and Contractor Employees although not part of the OPM's information technology is the best and "**LAST LINE OF DEFENSE**". When all layers fail and a cyber-attack is attempted or successful it is this defense layer where the attack is identified, acted on, and reported.

RESPONDING TO CYBER-ATTACKS

You won't be able to spot every potential cyber-attack, but when an attack occurs you should be ready to act.

PREPARE

Although most cyber-attacks will be stopped through cybersecurity software and tools (e.g. anti-virus, Virtual Private Networks, disk encryption, spam filtering, etc.) there always will be some cyber-attack that gets past these cybersecurity mechanisms. This is why you are a critical part of the effort to stop a cyber-attack.

At some point in your career as a federal or contractor employee you will encounter some form of a cyber-attack. Most cyber-attacks are successful because an individual failed either to follow the guidance provided or did not properly respond to identify, act, or report the cyber-attack.

Take some time to review the Cyber-Defense Prepare - Do's and Don'ts in this lesson to get a good idea of what you should do and not do.

IDENTIFY

As identified in the INTRODUCTION Lesson, "**OUR FIRST LINE OF DEFENSE IS OUR EMPLOYEES**".

The most critical part of the process is the identification of when a cyber-attack occurs or has already occurred.

Take some time and review the "**IDENTIFY A CYBER-ATTACK**" Section of this lesson

ACT

If you encounter a cyber-attack or suspect that a cyber-attack has already occurred **REMAIN CALM** and stop further activities until you document and report the cyber-attack.

Attempt to document what you encountered (what happened and time) for later investigation.

Once you report the cyber-attack you will be given further actions to take.

If the cyber-attack is a Phishing Attempt and you are using the OPM Microsoft Outlook you can, with the suspected email highlighted or open, click the "**Home**" Tab in the upper Menu, then select the "**Report Phishing**" Button in the menu bar.

REPORT

The final step is to report the cyber-attack. It is critical that any identified cyber-attack is reported immediately so that action can be taken to prevent others from encountering the same threat or reduce the overall impact to the agency and its information resources.

To report a cyber-attack, contact the Security Operations Center (SOC) at the following:

EMAIL: [redacted]@opm.gov

PHONE: 844-[redacted]

Follow the instruction given to you by the SOC.

Once reported to the SOC, then contact your supervisor and inform them of the situation.

PREPARE - CYBER-DEFENSE DO

Whenever you access an OPM information system keep in mind the following general **DO** in relation to use of information systems:

- *Do follow security procedures,*
- *Do report security problems, incidents, and suspicious or unusual behavior,*
- *Do recognize the accountability assigned to your User ID and password,*
- *Do log out or lock your workstation before leaving it unattended,*
- *Do limit personal use of your system, especially email and the Internet,*
- *Do keep your laptop and other personal electronic devices safe while traveling,*
- *Do ensure "need to know" before sharing information,*
- *Do shred sensitive documents before disposal.*

PREPARE - CYBER-DEFENSE DON'T

Whenever you access an OPM information system keep in mind the following general things to **DON'T DO** in relation to use of information systems:

- *Do not use a computer to harm other people,*
- *Do not interfere with other people's computer work,*
- *Do not snoop in other people's files,*
- *Do not use a computer to steal,*
- *Do not use or copy software you have not purchased, or have not been approved by the Agency,*
- *Do not steal other people's intellectual property or violate copyright laws,*
- *Do not use a computer to pose as another person,*
- *Do not use other people's computer resources without approval,*
- *Do not share your user ID and password,*
- *Do not install freeware and shareware that has not been tested and authorized for use by your Agency,*
- *Do not allow yourself to be a victim of social engineering or a scam by giving out information to unauthorized individuals.*

PREPARE - MULTIFACTOR AUTHENTICATION

Multi-factor authentication means the use of two out of the following three forms of authorization:

- Something you know (such as a password)
- Something you have such as a PIV card (You will need to know the PIN number associated with your PIV card)
- Something you are (biometric, such as fingerprint, eye)

PREPARE - MAINTAIN YOUR PIV CREDENTIAL

Like your driver's license or credit cards, you are responsible for protecting and caring for the Personal Identity Verification (PIV) Credential. Protective measures you need to take are:

- Keep your Credential in the government-issued badge holder when not in use. These badge holders are specially designed to protect your Credential. Other

containers and plastics, including your wallet, can damage or cause deterioration of the Credential.
- Do not punch holes, bend, mark, or peel any plastic away from the card.
- Do not scratch the magnetic stripe.
- Avoid storing your Credential in areas of extreme heat (e.g., clothes dryer) or sunlight (e.g., car dashboard) as the card could warp.
- Do not allow your Credential near magnetic fields (e.g., stereo equipment, magnets, other magnetic strip cards).
- Do not allow anyone else to use your PIV Credential under any circumstances.

PREPARE - PASSWORDS AND SECRET QUESTIONS

CREATING STRONG PASSWORDS

In some circumstances you will be asked to use some form of authentication other than using your PIV. This mostly will be a Username and Password combination that will let you gain access to information resources and capabilities. Use the following criteria for the development of a Strong Password:

- At least 8 Characters comprised of at least 1 Uppercase Letter, 1 Lowercase Letter, 1 Number, and 1 Special Character (not a letter or number). Privileged accounts require at least 12 characters.
- Should not contain any portion of the account Username or your name.
- Should not contain any common dictionary words.
- Should not contain simple patterns, such as keyboard "qwerty".
- Should not contain variations of the word "password" (.e.g. "P@ssw0rd!").
- Should not be a password that is being used for another application password.

CREATING STRONG SECRET QUESTIONS

In some circumstance you will be asked to create Secret (Golden) Questions that will be used to restore your Password in the event that a reset is necessary. Use the following criteria to Secret Questions:

- At minimum 3 Secret Questions should be created. More than three Security Questions should be created to allow for the rotation of Secret Questions for resets.
- When used for a Password Reset at least 3 Secret Questions must be successfully answered to allow the reset.

- **Safe** - The answers can't be easily guessed or researched.
- **Stable** - The response will not change - Example: Where did you lose your first tooth? Will always be answered: At Aunt Jane's house.
- **Memorable** - So you won't forget it.
- **Definitive/Simple** - Something that requires a specific answer that has a number of answers (e.g. What month did you graduate, there are only 12 months, and most graduations occur from May or June).

PREPARE - SENSITIVE DATA PROTECTION

Sensitive data is that for which loss, unauthorized modification, or unauthorized disclosure would be detrimental to national security operations and generally includes information that meets one or more of the following criteria:

- **Personal in Nature** - Social security numbers, medical information
- **Proprietary** - Contract proposals
- **Financial** - Procurement data
- **National Security Related** - Nuclear power plant blueprints
- **Critical to Agency Plans and Operations** - Network diagrams, password files
- **Shared Agency Information** - Information entrusted to OPM from other Federal Agencies.

All sensitive data must be password protected and kept in a secure place. Care should be exercised concerning the visibility of your computer screen to "over-the-shoulder" viewing, and the proximity of your work area to windows. Additionally, when leaving your desk, you should log off or lock your workstation, and exercise care about leaving sensitive papers on your desk.

Any mobile media (e.g. USB Flash Drives, CD-R, etc.) must be encrypted utilizing FIPS 140-2 validated encryption. In addition, encrypt any sensitive data before sending it electronically. Sensitive data that must be sent via email must be encrypted by typing the words "Send Secure" within the Subject line of the Outlook email. For further information about sending secure email, contact the OPM Help Desk.

PROTECTION OF IRS TAX INFORMATION

In addition to OPM Data Protection Guidance, U.S. Internal Revenue Service (IRS)Tax Information should be protected in accordance with the IRS Publication 1075, "Tax Information Security Guidelines For Federal, State and Local Agencies."

PREPARE - REGULAR BACKUPS

Regular backups minimize data loss from hard drive crashes, virus infections, and so forth. Consequently, you must ensure your files are backed up. You can ask your Help Desk or system administrator for assistance or if you have questions.
Additionally, here are a few backup tips for keeping your files adequately protected:

- *When editing a file create a copy so that you have a copy of the original.'*
- *Identify important files and documents and save them to a Networked Drive.*
- *When collaborating on a file or document utilize "Track Changes" so that you can revert to the original file/document.*
- *If large collaborations use a networked application like SharePoint.*
- *Any documents or information saved on the network drive will be automatically backed up on the network.*

PREPARE - PERSONNEL SECURITY

Personnel security reduces risks through procedures for position staffing and user administration. This ensures role-based and need-to-know access to the system. Personnel security includes, but is not limited to, the following:

- Background screening of job applicants and employees
- Need-to-know access based on job function
- Continual monitoring of employee system usage
- Separation of job duties

PREPARE - TELEWORK

With increased telework it is important to follow these procedures when working with PII data, using a computer or device external to OPM:

CONNECTIONS

- Work in a private location where information that you will be using is not visible to others
- Only use approved equipment to connect to OPM Information Systems and Information
- Connect to OPM Information Systems and Information through approved connections

INFORMATION RESOURCES

- Encrypt any PII data that is stored locally on the computer or device being used to telework
- Follow OPM policies for deleting PII data stored on a computer or device external to OPM to ensure the data is permanently deleted and not recoverable
- Do NOT print out PII data unless previously authorized and the ability to secure, or lock up, any hard copies and shred as necessary
- Do NOT discuss PII data in an environment where you can be overheard

PREPARE - NETWORK CONNECTIVITY

Part of telework is the connection to OPM Information Systems and Information. Use these methods to make a secure connection:

CONNECTING TO A HOME NETWORK

The Help Desk will ensure that your wireless device is working properly on your laptop when you bring it to the Help Desk for configuration and/or troubleshooting. However, because of the number of wireless network devices and numerous configuration options, the OPM Help Desk cannot set up or trouble-shoot individual home network configurations. OPM employees should take the following steps to make sure their home networks are configured correctly and securely:

- Modern wireless equipment for the home, such as Wi-Fi routers, has the capability to be secured. Each device manufacturer has different ways of implementing these security controls, but they all conform to a common set of standards (such as Wi-Fi Protected Access, or WPA).
- OPM employees who wish to use their home wireless networks to access OPM resources should refer to their equipment documentation to make sure they have taken steps to protect their network. Internet Service Providers may also have support phone numbers that employees can call to get assistance securing their wireless home networks.
- Do not share passwords, keys, PINS or other information about home wireless networks with anyone.
- Change device passwords periodically and do not use default passwords set by equipment manufacturers.
- Do not allow anyone, including family members, to use OPM-issued equipment for any reason.
- When you step away from your computer at home, just like you would at work, make sure to lock the system or log off so that no one can use it without your knowledge or permission.

- During setup of wireless equipment at home, always select the option that requires a heightened level of security and password. Do not configure wireless devices so that anyone can access without permission or a password or passphrase.

CONNECTING TO A THIRD-PARTY NETWORK

There are Wi-Fi networks almost everywhere you go these days. Many of these are managed by retail companies that want to provide the service as a way to attract customers. It is extremely important that you know who is running a wireless network before you connect to it. Here are some steps you should follow to make sure you connect securely:

- Do not connect to a wireless network if you are not sure who is running it. For example, if you are in a coffee shop, you may see several Wi-Fi network names when you use your computer. You should only connect to the network run by that coffee shop; if you are not sure which network is the right one, either do not connect at all or ask an employee.
- When traveling, the hotel where you stay may provide wireless access. Often, in order to use these networks, you must verify that you are a guest of the hotel by providing a key or other information. As with the coffee shop example above, make sure to verify with the hotel the proper network and the right procedures.
- It is your responsibility to practice safe computing. Third party wireless networks may be run by someone trying to get access to your Personal Information or other information on your computer. If you are not sure who is managing a wireless network, do not use it!

PREPARE - ENCRYPT SENSITIVE EMAILS

To meet our analysis requirements, all encrypted files and attachments sent or received by our OPM email systems are blocked and quarantined. Such files include password-protected attachments. Commonly encrypted files include PDFs, WinZip files, and Microsoft Office documents. To manage such files, employees should use the following guidelines:

- When emailing encrypted files to approved external recipients, use OPM's enterprise secure messaging portal. For information about this secure method of file transfer, contact: [redacted]@opm.gov or the OPM Help Desk Self Help web page on the OPM intranet (THEO).
- When you need to receive an encrypted file from an approved external sender, contact [redacted]@opm.gov. Cybersecurity will perform validation and risk-assessment tasks in order to facilitate a secure transfer of the file.

If you have questions about the secure messaging portal or transferring encrypted files, please email [redacted]@opm.gov.

IDENTIFY AN EMAIL CYBER-ATTACK

Most cyber-attacks that you will encounter will come from an unsolicited email. These emails will contain some form of mechanism or method (e.g. Social Engineering) to circumvent implemented cybersecurity mechanisms. Some of these include:

Suspicious Emails: Emails from a known or unknown sender with misspellings or asking for unrelated work information or giving instructions to view or download files that were not asked for or not related to a work activity (e.g. "pictures of my vacation"). Look at the FROM: address; the TO: address (is it directly to you or a large group of people); SUBJECT: line; time of day it was sent; and content to misspellings, hyperlinks, and attachments.

Suspicious Hyperlinks: A link in an email that does not go to the correct site as described by the link or that is directed to an unauthorized/unwanted web site such as an unsolicited link to update your account information.

Suspicious Attachments: Attachments that were not requested especially those coming externally from someone other than a co-worker or someone known to you.

Sent Emails: It is a good idea to periodically check your "Sent Mail" Folder to see if there are emails that you did not send. This is a good sign that your email account or application has been compromised.

IDENTIFY AN INTERNET CYBER-ATTACK

Surfing the internet, even an authorized government website, may lead you to internet sites that can initiate a cyber-attack. Some internet things to look out for:

Pop-Ups: Unwarranted pop-ups are not only a nuisance they can be a sneaky way to get you to click on some ad or some other mechanism to redirect you to a nefarious website.

Redirection: In most circumstances you will be notified that you are leaving a website. During a redirection (e.g. going from opm.gov to irs.gov or to another website) if there is a change in the URL root domain (e.g. opm.gov) this may be a cause for alarm.

Installs: When you are asked to install anything (software, plug-ins, add-ons, widgets, etc.) you should not accept. Any installation of software to include browser add-ons and plug-ins, must be approved and performed by the OPM Help Desk or authorization System Administrator.

Reauthentication: In some circumstances you may be required to re-authenticate your credentials when accessing information resources. When asked to provide access credentials assure that the website is an "official" site, and the URL prefix is "https" (a secure website). An unexpected request to provide credentials may be an attempt to capture your login information.

If the website address is something other than what you expect (e.g. an IP Address instead of a URL Address, a .com instead of a .gov) this may be a redirection to an attackers' web page. Also, in some circumstances websites will ask you to load some kind of "plug-in" or "widget" to view the information, create an account, or allow access to your personal computer resources.

IDENTIFY A PHONE CYBER-ATTACK

Although most attempts will come from email and the internet, some threat sources still use the phone (line or cell) to initiate their Social Engineering cyber-attack. These methods include:

Scams: Most phone cyber-attacks are in the form of scams to get you to perform actions based on an urgent need. For instance, this scam, "A call from a person at the IRS stating you owe them money and if you do not pay them immediately, they will issue a warrant for your arrest". This scam usually includes you giving them bank information or going to Western Union to send money to prevent you from being arrested.

Quid Pro Quo: This cyber-attack like a scam offers you something, a prize or money, however, to get it you must pay a fee for processing or effort to deliver. For instance, this may be a call saying that you have inherited a large sum of money and that in order for them to transfer it to you to send them a processing fee.

Vishing: An attacker can perpetrate a vishing campaign by setting up a Voice over Internet Protocol (VoIP) server to mimic various entities in order to steal sensitive data and/or funds.

Impersonation: A common cyber-attack is someone pretending that they are someone that you would normally trust. This trust is used to solicit information from you that could be used in a cyber-attack. For example, someone calls and says they are from the helpdesk, and they received an alert that you have a computer-virus on your PC. They then ask you to authenticate your information so that they can initiate a repair to remove the virus.

Notifications: These are in the form of an alert that someone has broken into your banking account or is charging to your credit card. The person will then ask you to provide your banking or credit card information to verify your account.

IDENTIFY AN IN PERSON CYBER-ATTACK

Although not the preferred method, some cyber-attacks can occur during a direct interaction with a person (someone known or unknown). These interactions prey upon your courtesy and generosity. A common cyber-attack would be a person with their hand full asking you to hold the door open or open the door to a card-access area, like a data center or building that they do not have access to. These types of attacks include:

Impersonator: Similar to other attacks an individual is pretending that they are someone that you would normally trust. This trust is used to solicit information from you that could be used in a cyber-attack.

Borrower: This individual poses as someone that needs help in accessing some resource. They use excuses (my computer is updating, I left my laptop at home, I keep getting an error accessing the website, etc.) to borrow your information resource (computer, phone, etc.) for a short period of time. This not only gives them access to all the resources that you have access to but also leaves an audit trail based on your ID.

Hapless Victim: This individual acts as they are in dire straits and need your assistance. An example is someone carrying coffee and donuts for the entire office asking the security guard to let them in because their hands are full, and they cannot retrieve their credentials.

IDENTIFY A CYBER-ATTACK, KEY AWARENESS

Not all indicators are related to a direct cyber-attack, some are performed in the background without your knowledge or any initial indicator that the cyber-attack occurred. Some things to be aware of are:

Unusual Activities/Actions: Be aware of some actions or activities that were not initiated by you, such as emails in your "Sent Items" email box that were not sent by you.

Resource Availability: Some resources that were previously accessible are no longer accessible because of a permissions change or change to your credentials. This would also include additional access to resources that you did not request access to or should not have access to, based on work requirements. Also, if information previously stored has been altered or deleted without your knowledge.

Resource Abnormal Behaviors: Some of the resources you are utilizing are acting/behaving abnormal, like your email is slow/sluggish, routine auto-actions are not being performed, like backups or archiving of data. Another is unaware connections to resources other than your own (wireless, Bluetooth, etc.).

Lesson 5

ACKNOWLEDGEMENT

ACKNOWLEDGEMENT OF OPM's SECURITY POLICY AND RULES OF BEHAVIOR

I understand that, when using the OPM Network, I am personally accountable for my actions and must comply with the Rules of Behavior.

I understand the policy is based on Federal laws, regulations, and OPM directives and policies. As such, I understand there are consequences for non-compliance with OPM's Security Policy and Rules of Behavior. Depending on the severity of the violation, at the discretion of management and through due process of the law, consequences can include suspension of access privileges, reprimand, suspension from work, demotion, dismissal, and/or criminal and civil penalties. For any questions regarding the Information Security and Privacy Policy, please email [redacted]@opm.gov.

I also understand that OPM's computers, networks, and information systems are not "private", and I should have no expectation of privacy when using OPM's computing resources, which is reiterated in OPM's IT System Security Warning Banner. I understand management has the right to monitor, intercept, read, record, and copy information attributable to my access of these resources.

From: Rowell, Danielle R
To: Greg Hogan; Garcia, Carmen E.
Subject: Re: Welcome to OPM - Instructions Prior to Onboarding
Attachments: image001.png

Hi Greg,

Received. Thank you.

Get Outlook for iOS

From: Greg Hogan [redacted]>
Sent: Monday, January 20, 2025 10:24:11 AM
To: Garcia, Carmen E. <[redacted]@opm.gov>; Rowell, Danielle R <[redacted]@opm.gov>
Subject: Re: Welcome to OPM - Instructions Prior to Onboarding

I have completed the Cybersecurity and Privacy Awareness Training.

Thanks!
Greg Hogan

On Sat, Jan 18, 2025 at 3:33 PM Garcia, Carmen E. <[redacted]@opm.gov> wrote:

> Good Afternoon,
>
> It gives us immense pleasure to welcome you to our OPM team! We are excited to have you start on Monday and look forward to the valuable contributions we know you will make.
>
> To ensure a smooth transition, we have a few key items for you to review.
>
> ## Training Requirements:
>
> We have attached the OPM cybersecurity training course document for your review. This will provide you with fundamental knowledge about your responsibilities in safeguarding OPM's information systems and resources. Kindly take a moment to go through it before Monday. Once done, please send a confirmation email to Danielle Rowell, our Acting Chief Information Security Officer, at [redacted]@opm.gov, acknowledging that you have understood the contents.
>
> ## Directions to OPM:
>
> Given the traffic patterns, driving to the Theodore Roosevelt Building can be challenging. However, if you decide to use your personal vehicle, we've arranged a parking pass for you at the guard house on the 20th Street entrance. We've also attached a local public safety map for your convenience. If you prefer not to drive, simply come to the E St. main entrance, where you will be warmly welcomed and escorted into the building.
>
> ## Essentials to Bring:

Please remember to bring along a valid U.S. Passport and a voided check.

We are excited to welcome you to the OPM family and eagerly await your arrival on Monday. If you have cleared security, you will receive or have received a final job offer letter with instructions to complete new hire paperwork. If you are not able to clear before Monday, we will help you complete the forms on Monday. Should you encounter any difficulties in reaching the building, please feel free to reach out to me via call or email.

Have a wonderful weekend!

Carmen

Carmen E. Garcia

CHIEF HUMAN CAPITAL OFFICER | HUMAN RESOURCES DIRECTOR

Office of the Chief Human Capital Officer | U.S. Office of Personnel Management

1900 E St. NW | Washington DC 20415
Office: (202) [redacted]

For scheduling, please contact: [redacted]@opm.gov

OPM.gov

Follow us on LinkedIn | Twitter | YouTube

From: Rowell, Danielle R
To: OPM-7 ; Garcia, Carmen E.
Subject: Re: completed cybersecuirty training, OPM-7

Hi OPM-7,
Received. Thank you.

Get Outlook for iOS

From: OPM-7 <[redacted]>
Sent: Sunday, January 19, 2025 9:51:03 AM
To: Rowell, Danielle R <[redacted]@opm.gov>
Cc: OPM-7 <[redacted]>
Subject: completed cybersecuirty training, OPM-7

You don't often get email from [redacted]. Learn why this is important

Hi Danielle- I finished the cybersecurity training that was sent to me and was asked to let you know once completed. Thank you!

Regards,
OPM-7

From: Rowell, Danielle R
To: OPM-5
Cc: Garcia, Carmen E.; Saunders, James L
Subject: Re: OPM Security Course

Hi OPM-5,

Received. Thank you.

Get Outlook for iOS

From: OPM-5 <[redacted]>
Sent: Saturday, January 18, 2025 6:06 PM
To: Rowell, Danielle R <[redacted]@opm.gov>
Subject: OPM Security Course

You don't often get email from [redacted] Learn why this is important

Hello Danielle,

I have read and understood OPM cybersecurity training.

Thanks,
OPM-5

From: Rowell, Danielle R
To: OPM-2
Cc: Garcia, Carmen E.
Subject: Re: OPM Cybersecurity training - confirmation of completion

Hi OPM-2,

Received. Thank you.

Get Outlook for iOS

From: OPM-2 [redacted]>
Sent: Sunday, January 19, 2025 2:12:27 PM
To: Rowell, Danielle R <[redacted]@opm.gov>
Cc: Garcia, Carmen E. <[redacted]@opm.gov>
Subject: OPM Cybersecurity training - confirmation of completion

Dear Danielle Rowell,
Per request from Carmen Garcia (in CC), this email is to confirm that I have reviewed and understood the document "OPM Cybersecurity And Privacy Awareness Training".

Best regards,
OPM-2

From: Personnel Security Group
To: Sylke, Kimberly D.
Cc: Lowe, Dana S.; Nickerson, Tiffany V.; Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Duncan, Jennifer
Subject: OPM-2 - CLEARED 01/20/2025
Date: Monday, January 20, 2025 2:40:00 PM
Attachments: image001.png

Please note that this cleared message is for a temporary appointment for less than 180 days.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) [redacted] | OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Dillaman, Miranda C.
To: Sylke, Kimberly D.
Subject: RE: Documentation for Transition Team - OPM-2
Date: Monday, January 20, 2025 2:24:00 PM
Attachments: image002.png

Thanks Kim!

Nothing further is needed at this time. You will receive a separate EOD message.

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) [redacted] | OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Sylke, Kimberly D. <[redacted]@opm.gov>
Sent: Monday, January 20, 2025 2:09 PM
To: Dillaman, Miranda C. <[redacted]@opm.gov>
Subject: Fw: Documentation for Transition Team - OPM-2

From: Riccardo Biasini [redacted]>
Sent: Monday, January 20, 2025 1:38 PM
To: Sylke, Kimberly D. <[redacted]@opm.gov>
Subject: Fwd: Documentation for Transition Team - OPM-2

Hi Kimberly,
See signed docs attached.

Best,
OPM-2

---------- Forwarded message ---------
From: OPM-2 [redacted]>
Date: Thu, Jan 16, 2025 at 11:50 AM
Subject: Documentation for Transition Team - OPM-2
To: <[redacted]@opm.gov>

Dear Carmen Garcia,
This is OPM-2 , appointee for an employment in the Federal Employment.
Attached you can find:

- My CV
- Signed OF 306
- Signed SF 86

Please don't hesitate to reach out to me in case you need anything else.

Best regards,
OPM-2

From: Dillaman, Miranda C.
To: Sylke, Kimberly D.
Cc: Beckman, Christopher J.; Davis, Melinda M.; Hazlett, Amber L.
Subject: RE: Converting to Permanent Appointment
Date: Wednesday, March 19, 2025 7:16:00 AM
Attachments: image002.png

Thanks Kim!

OPM-2 will need a full investigation on the 86. Fingerprints are not needed. I will take care of the eApp, email and cc you.

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) [redacted] | OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Sylke, Kimberly D. <[redacted]@opm.gov>
Sent: Tuesday, March 18, 2025 4:32 PM
To: Dillaman, Miranda C. <[redacted]@opm.gov>
Cc: Beckman, Christopher J. <[redacted]@opm.gov>; Davis, Melinda M. <[redacted]@opm.gov>; Hazlett, Amber L. <[redacted]@opm.gov>
Subject: Converting to Permanent Appointment

Hi Miranda,

I verified the following appointee will move to permanent position:

- OPM-2 (Expert)

He will be on the same PD, please let me know if you need any additional information.

V/R

Kim

SUPERVISORY HR SPECIALIST, EXECUTIVE RESOURCES

Office of the Chief Human Capital Officer | U.S. Office of Personnel Management

1900 E. St. NW | Washington DC 20415

Office: (202) [redacted]

Email: [redacted]@opm.gov

From: Personnel Security Group
To: Sylke, Kimberly D.
Cc: Lowe, Dana S.; Nickerson, Tiffany V.; Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Duncan, Jennifer
Subject: OPM-7 - CLEARED 01/17/2025
Date: Friday, January 17, 2025 7:25:00 AM
Attachments: image001.png

Please note that this cleared message is for a temporary appointment for less than 180 days.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) [redacted] | OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Dillaman, Miranda C.
To: Sylke, Kimberly D.
Cc: Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Lowe, Dana S.; Nickerson, Tiffany V.
Subject: RE: New Hire Information for Incoming Senior Advisor to the Director
Date: Thursday, January 16, 2025 12:04:00 PM
Attachments: image002.png
image003.png

Hi Kim!

I've been notified that OPM-7 has been fingerprinted today. Nothing further is required at this time. You will receive a separate EOD message.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) [redacted] OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Sylke, Kimberly D. <[redacted]@opm.gov>
Sent: Thursday, January 16, 2025 11:41 AM
To: Dillaman, Miranda C. <[redacted]@opm.gov>
Cc: Garcia, Carmen E. <[redacted]@opm.gov>; Beckman, Christopher J. <[redacted]@opm.gov>; Davis, Melinda M. <[redacted]@opm.gov>; Lowe, Dana S. <[redacted]@opm.gov>; Nickerson, Tiffany V. <[redacted]@opm.gov>
Subject: New Hire Information for Incoming Senior Advisor to the Director

Good Morning Miranda,

Requesting temporary clearance (less than 180 days) for OPM-7 , incoming Senior Advisor to the Director. Attached are the required documents for your review.

Please let me know if you need any additional information.

V/R

Kim

Kim Sylke (pronouns: she/her)

SUPERVISORY HR SPECIALIST, EXECUTIVE RESOURCES

Office of the Chief Human Capital Officer | U.S. Office of Personnel Management

1900 E. St. NW | Washington DC 20415

Office: (202) [redacted]

Email: [redacted]@opm.gov

OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | X | YouTube

From: Personnel Security Group
To: Sylke, Kimberly D.
Cc: Lowe, Dana S.; Nickerson, Tiffany V.; Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Duncan, Jennifer; Phillips, Keith; Mitchell, Diana; Hazlett, Amber L.
Subject: OPM-7 - CLEARED 01/31/2025
Date: Friday, January 31, 2025 1:28:00 PM
Attachments: image002.png

**Please note that this cleared message is for a permanent position over 180 days. The individual was previously cleared for less than 180 days.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) [redacted] | OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Dillaman, Miranda C.
To: Sylke, Kimberly D.
Cc: Davis, Melinda M.; Mitchell, Diana; Hazlett, Amber L.; Nickerson, Tiffany V.; Lowe, Dana S.; Dennis, Natasha
Subject: RE: Permanent PIV Request for OPM-7
Date: Thursday, January 30, 2025 8:00:00 AM
Attachments: image002.png

Hi Kim!

We will be reviewing a previous investigation from OPM-7 . Nothing further is required at this time. You will receive a separate EOD message.

Thanks!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) [redacted] | OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Sylke, Kimberly D. <[redacted]@opm.gov>
Sent: Wednesday, January 29, 2025 5:00 PM
To: Dillaman, Miranda C. <[redacted]@opm.gov>
Cc: Davis, Melinda M. <[redacted]@opm.gov>; Mitchell, Diana <[redacted]@opm.gov>; Hazlett, Amber L. <[redacted]@opm.gov>; Nickerson, Tiffany V. <[redacted]@opm.gov>; Lowe, Dana S. <[redacted]@opm.gov>; Dennis, Natasha <[redacted]@opm.gov>
Subject: Permanent PIV Request for OPM-7

Hi Miranda,

Requesting a permanent PIV for Expert OPM-7 . Attached are following documents for your review:

- Resume
- PD
- New Hire Information

Please let me know if you need additional information and/or documents.

Thank you,
Kim

From: Personnel Security Group
To: Sylke, Kimberly D.
Cc: Lowe, Dana S.; Nickerson, Tiffany V.; Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Duncan, Jennifer
Subject: OPM-3 - CLEARED 01/20/2025
Date: Monday, January 20, 2025 1:48:00 PM
Attachments: image001.png

Please note that this cleared message is for a temporary appointment for less than 180 days.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202)[redacted] | OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Dillaman, Miranda C.
To: Sylke, Kimberly D.
Cc: Lowe, Dana S.; Nickerson, Tiffany V.
Subject: RE: Documents for OPM
Date: Monday, January 20, 2025 11:44:00 AM
Attachments: image002.png

Thanks Kim!

We will just need fingerprints for OPM-3 (which I'm sure he is set to be printed). You will receive a separate EOD message.

Thanks!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) [redacted] | OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Sylke, Kimberly D. <[redacted]@opm.gov>
Sent: Monday, January 20, 2025 11:39 AM
To: Dillaman, Miranda C. <[redacted]@opm.gov>
Cc: Lowe, Dana S. <[redacted]@opm.gov>; Nickerson, Tiffany V. <[redacted]@opm.gov>
Subject: Fw: Documents for OPM

Hi Miranda, here's a hot one

Still trying to figure where this individual will work, I'll send as soon as I can.

V/R
Kim

From: Garcia, Carmen E. <[redacted]@opm.gov>
Sent: Monday, January 20, 2025 11:11 AM
To: Sylke, Kimberly D. <[redacted]@opm.gov>
Subject: Fw: Documents for OPM

Please send to security and I need a folder, label, and a tent for him please

Get Outlook for iOS

From: Garcia, Carmen E.
Sent: Sunday, January 19, 2025 8:22:08 PM

To: Malague, Katie <[redacted]@opm.gov>
Subject: FW: Documents for OPM

Hi Katie,

I am not tracking this person. Are you aware of him?

Thanks,
Carmen

From: OPM-3 <[redacted]>
Sent: Sunday, January 19, 2025 5:22 PM
To: Garcia, Carmen E. <[redacted]@opm.gov>
Subject: Documents for OPM

You don't often get email from [redacted]. Learn why this is important

Hi Carmen,

It's great to meet you! I've been told to reach out to you with the following documents for employment at OPM. I have attached them below, please let me know if you need anything else from me.

Thanks,
OPM-3

From: Personnel Security Group
To: Sylke, Kimberly D.
Cc: Lowe, Dana S.; Nickerson, Tiffany V.; Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Duncan, Jennifer
Subject: OPM-4 - CLEARED 01/24/2025
Date: Friday, January 24, 2025 10:45:00 AM
Attachments: image001.png

Please note that this cleared message is for a temporary appointment for less than 180 days.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) [redacted] | OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Davis, Melinda M.
To: Beckman, Christopher J.
Cc: Dillaman, Miranda C.
Subject: FW: Rush on Onboarding
Date: Friday, January 24, 2025 7:55:51 AM
Attachments: Outlook-m20yup3t.png
image003.png

Chris-
We have no record fingerprints but we do not have the 306 or release. Kim is supposed to be reaching out this morning to obtain these. That is the latest status we have. As soon as we get the paperwork we can clear. Thanks.

Mindy Davis | Division Director-Personnel Security

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management
M: (202) [redacted] | OPM.gov
T: (202)
OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Hilliard, Everette <[redacted]@opm.gov>
Sent: Friday, January 24, 2025 5:54 AM
To: Davis, Melinda M. <[redacted]@opm.gov>; Dillaman, Miranda C. <[redacted]@opm.gov>; Beckman, Christopher J. <[redacted]@opm.gov>
Subject: Fwd: Rush on Onboarding

Sent from my iPhone

Begin forwarded message:

> **From:** "Garcia, Carmen E." <[redacted]@opm.gov>
> **Date:** January 23, 2025 at 10:07:38 PM EST
> **To:** "Ezell, Charles E." <[redacted]@opm.gov>, "Hilliard, Everette" <[redacted]@opm.gov>
> **Cc:** OPM-7 @opm.gov>
> **Subject: Re: Rush on Onboarding**
>
> Good Evening Acting Director,
>
> I will prioritize this and make sure we see this through expeditiously. We just need to execute an MOU and it's drafted and signed on our end. I just need to get in touch with their respective agencies for their signature in order to finalize the detail.

We hope to have resolution early tomorrow.

Thank you,
Carmen

Get Outlook for iOS

From: Ezell, Charles E. <[redacted]@opm.gov>
Sent: Thursday, January 23, 2025 10:04:32 PM
To: Garcia, Carmen E. <[redacted]@opm.gov>; Hilliard, Everette <[redacted]@opm.gov>
Cc: OPM-7 @opm.gov>
Subject: Rush on Onboarding

Reid & Carmen, we need to quickly onboard the two DOGE employees tomorrow if at all possible. I'm not sure where they are in the process but we are desperately needing their engineering skills to help with a special project for President Trump.

- OPM-4
- OPM-6

.ce

Chuck Ezell

Acting Director

U.S. Office of Personnel Management

(478) [redacted]

[redacted]@opm.gov

OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Personnel Security Group
To: Sylke, Kimberly D.
Cc: Lowe, Dana S.; Nickerson, Tiffany V.; Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Duncan, Jennifer
Subject: HOGAN, Gregory - CLEARED 01/14/2025
Date: Tuesday, January 14, 2025 12:18:00 PM
Attachments: image002.png

Please note that this cleared message is for a temporary appointment for less than 180 days.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) [redacted] | OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Dillaman, Miranda C.
To: Sylke, Kimberly D.
Cc: Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Pettit, John; Lowe, Dana S.; Nickerson, Tiffany V.
Subject: RE: New Hire Information for Incoming Senior Advisor to the Director (Hogan)
Date: Monday, January 13, 2025 2:35:00 PM
Attachments: image003.png
image002.png

Hi Kim!

Greg Hogan will need fingerprints (which I have been notified he came in for fingerprinting today). You will receive a separate EOD message.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: [redacted] | OPM.gov

U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Sylke, Kimberly D. <[redacted]@opm.gov>
Sent: Monday, January 13, 2025 2:03 PM
To: Dillaman, Miranda C. <[redacted]@opm.gov>
Cc: Garcia, Carmen E. <[redacted]@opm.gov>; Beckman, Christopher J. <[redacted]@opm.gov>; Davis, Melinda M. <[redacted]@opm.gov>; Pettit, John <[redacted]@opm.gov>; Lowe, Dana S. <[redacted]@opm.gov>; Nickerson, Tiffany V. <[redacted]@opm.gov>
Subject: New Hire Information for Incoming Senior Advisor to the Director (Hogan)

Good Afternoon Miranda,

Requesting temporary clearance (less than 180 days) for Greg Hogan, incoming Senior Advisor to the Director. Attached are the required documents for your review.

Please let me know if you need any additional information or have any questions.

V/R

Kim

Kim Sylke (pronouns: she/her)

SUPERVISORY HR SPECIALIST, EXECUTIVE RESOURCES

Office of the Chief Human Capital Officer | U.S. Office of Personnel Management

1900 E. St. NW | Washington DC 20415

Office: (202) [redacted]

Email: [redacted]@opm.gov

OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | X | YouTube

Stugart, Sarah B.

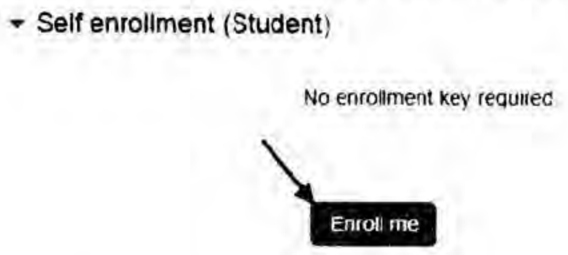
From:	Stugart, Sarah B.
Sent:	Thursday, March 6, 2025 2:10 PM
To:	Hogan, Greg
Subject:	Clearance-Hogan
Importance:	High

Good afternoon, Mr. Hogan,

As part of your duties with USOPM, it has been requested that you be granted access to Top Secret classified information. Additionally, it was further requested that you be processed for SCI access. The Top-Secret access is required to be granted prior to the SCI access and this email informs you of the requirements for the Top-Secret clearance access only. Once the Top-Secret clearance is in place you will be provided further instructions for the SCI access.

You are required to complete the on-line Classified National Security Awareness and Insider Threat Training located on the USOPM Learning Connection portal. The link to the training is: https://learningconnection.opm.gov/course/view.php?id=32655 Chrome Browser is recommended.

Access the OPM Learning Connection web site and locate the course. Directly below the course title will be an **Enroll Me** button that will allow you to self-enroll (see screen shot below). Once you click that button, you will receive an email stating that you are enrolled. You do not have to open the email or do anything with it. You should be able to click on the course's link to enter the training modules.



*If you do not see any of the above steps when you log on do a key word search for the course by typing or copying and pasting the following into the course search box: **CY 2024 Classified National Security Information Awareness and Insider Threat Training.** The course should now be displayed for you to choose.
You must complete the on-line training and pass it with a score of at least 80. After you complete the training, you must print your certificate. If you cannot obtain the certificate, please obtain a copy/snapshot of the actual test results. Send me a copy of your certificate/test results by email attachment to [redacted]@opm.gov. Upon receipt of the certificate, arrangements will be made to complete the SF 312, Classified Information Nondisclosure Agreement.

If you encounter any technical difficulties with the OPM Learning Connection, please refer to the website itself for instructions on how to contact the Help Desk.

If you have any questions regarding the clearance process, please let me know. Thank you.

Thank you.

Sarah Stugart | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
Phone: 202[redacted] | OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
INVESTIGATIONS SERVICE
WASHINGTON, DC 20415

CERTIFICATION OF INVESTIGATION

DATE: 03/05/2025

SUBMITTING OFFICE: SON - 133H SECURITY OFFICE: SOI - OM00

OPM
ATTN: CSEA
P.O. BOX 618
1137 BRANCHTON ROAD
BOYERS, PA 16018

NAME: HOGAN, GREGORY JOHN

SSN: [redacted] DOB [redacted] POSITION: CHIEF INFORMATION OF

CASE TYPE: T5 CLOSING DATE: 03/05/2025 OPM CASE #: 2509900333
EXTRA COVERAGE: L / BVS
3 / ADVANCED REPORT OF NAC
PT / PRESIDENTIAL TRANSITION CASES
POSITION CODE : /

SCHEDULED DATE: 02/06/2025

INVESTIGATION CONDUCTED FROM: SF86 (7/17)

THIS CERTIFIES THAT A BACKGROUND INVESTIGATION ON THE PERSON IDENTIFIED ABOVE HAS BEEN COMPLETED. THE RESULTS OF THIS INVESTIGATION WERE SENT TO THE SECURITY OFFICE FOR A SECURITY/SUITABILITY DETERMINATION.

****

AGENCY CERTIFICATION: THE RESULTS OF THIS INVESTIGATION HAVE BEEN REVIEWED, AND A FINAL DETERMINATION HAS BEEN MADE.

AGENCY CERTIFYING OFFICIAL SARA ARBLASTER Digitally signed by SARA ARBLASTER Date: 2025.03.06 11:46:16 -05'00' DATE

FILE THIS CERTIFICATE ON THE PERMANENT SIDE OF THE PERSON'S OFFICIAL PERSONNEL FOLDER AFTER THE FINAL AGENCY DETERMINATION IS MADE.

Personnel Security Group

From:	Personnel Security Group
Sent:	Thursday, March 6, 2025 12:55 PM
To:	Hogan, Greg
Subject:	Hogan, Gregory - NOTIFICATION OF COMPLETION OF INVESTIGATIVE PROCESS

Congratulations Mr. Hogan,

The background investigation for your employment with the U.S. Office of Personnel Management was favorably adjudicated by Personnel Security on March 6, 2025. Your investigation was favorably adjudicated under both 5 CFR 731, Suitability Guidelines and E.O. 12968, National Security Adjudicative Guidelines. If your position requires access to classified information, you are eligible to be processed for a security clearance equivalent to your Position Designation. You will be contacted separately by a member of the Personnel Security Staff to complete a security clearance briefing/training and to execute the SF 312 Non-disclosure Agreement prior to being granted access to classified information. If you have any questions regarding this notice or any other Personnel Security related matter, please contact me at the number below.

On October 1, 2019, as authorized by Executive Order 13869, the mission, records, and personnel of the OPM, National Background Investigations Bureau, transferred to the Department of Defense, Defense Counterintelligence and Security Agency (DCSA). Accordingly, as of October 1, 2019, in order to obtain a copy of your background investigation, request an amendment to your records, or file a FOIA request related to background investigation data or records, please follow the instructions at DCSA's website: https://www.dcsa.mil/mc/pv/mbi/mr/. If you have specific questions, you may contact the DCSA Freedom of Information and Privacy Office for Investigations at: (878)[redacted].

Thank you,

Sara Arblaster
Personnel Security Specialist
U.S. Office of Personnel Management
Facilities, Security & Emergency Management-Personnel Security
o: (202)[redacted]
f. (724)[redacted]
[redacted]@opm.gov
OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Personnel Security Group
To: Sylke, Kimberly D.
Cc: Lowe, Dana S.; Nickerson, Tiffany V.; Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Duncan, Jennifer; Hazlett, Amber L.; Mitchell, Diana
Subject: HOGAN, Gregory - CLEARED 02/10/2025
Date: Monday, February 10, 2025 1:12:00 PM
Attachments: image002.png

**Please note that this cleared message is for a permanent position over 180 days. The individual was previously cleared for less than 180 days.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) [redacted] | OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Dillaman, Miranda C.
To: Sylke, Kimberly D.
Cc: Davis, Melinda M.; Mitchell, Diana; Hazlett, Amber L.; Nickerson, Tiffany V.; Lowe, Dana S.; Dennis, Natasha
Subject: RE: Permanent - Greg Hogan (Noncareer SES) - Chief Information Officer
Date: Thursday, January 30, 2025 6:14:00 AM
Attachments: image002.png

Hi Kim!

Greg Hogan will need a full investigation on the 86. Fingerprints are not needed. I will take care of the eApp, email and cc you.

Thanks!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) [redacted] | OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Sylke, Kimberly D. <[redacted]@opm.gov>
Sent: Wednesday, January 29, 2025 4:07 PM
To: Dillaman, Miranda C. <[redacted]@opm.gov>
Cc: Davis, Melinda M. <[redacted]@opm.gov>; Mitchell, Diana <[redacted]@opm.gov>; Hazlett, Amber L. <[redacted]@opm.gov>; Nickerson, Tiffany V. <[redacted]@opm.gov>; Lowe, Dana S. <[redacted]@opm.gov>; Dennis, Natasha <[redacted]@opm.gov>
Subject: Permanent - Greg Hogan (Noncareer SES) - Chief Information Officer

Hi Miranda,

Requesting clearance to move Greg Hogan to a permeant Chief Information Officer (Noncareer SES) position. Attached are following documents for your review:

- Resume
- PD
- New Hire Information

Please let me know if you need additional information.

V/R
Kim

GSA USACCESS Program

Applicant Status Report **Report Print Date :** **04/14/2025** **12:47:51PM**

APPLICANT INFORMATION - Page 2

Enrollment ID [redacted] **Name** HOGAN GREGORY JOHN **DOB** [redacted]

ADJUDICATION INFORMATION

Adjudication Status ADJUDICATED
Adjudication Create Date / Last Update 10-Feb-2025 13:12 / 07-Mar-2025 12:53
NCHC/FBI APPROVED **NCHC/FBI Adjudicator ID** [redacted]
NACI APPROVED **NACI Adjudicator ID** [redacted]
Adj Last Update Agency OFFICE OF PERSONNEL MANAGEMENT
Adj Last Update Agency Date 07-Mar-2025 12:53
PIV Agency Specific Criteria Status **PIV-I Agency Specific Criteria Status**
PIV Agency Specific Criteria Date **PIV-I Agency Specific Criteria Date**

ENROLLMENT INFORMATION

Enrollment Status COMPLETE **Last Enrollment Date** 10-Feb-2025 16:23
Enrollment Create Date 10-Feb-2025 13:12 **Enrollment Last Update** 10-Feb-2025 16:22
Document Referral NO
Enrollment Site ID/Description 102415 / OPM LCS 10
Enrollment Site Address: Line 1 1H17
Line 2 1900 E ST NW
Line 3
City /State / Zip Code WASHINGTON / DC / 20415

ISSUANCE INFORMATION

CURRENT CARD		REPLACEMENT CARD	
Issuance Status	ACTIVE	**Issuance Status**	NO STATUS
Create/Last Update Date	12-Feb-2025 16:33 / 13-Feb-2025 9:37	**Create/Last Update Date**	/
CMS Card ID	[redacted]	**CMS Card ID**	
Card ID	2 **Card Destroyed** NO	**Card ID**	
FASC-N	[redacted]	**FASC-N**	
Card UUID	[redacted]	**Card UUID**	
Issuance Sub-Status	ACTIVATED	**Issuance Sub-Status**	NO STATUS
Issuance Cred Option	PIV	**Issuance Cred Option**	
Certificate Set	4	**Certificate Set**	
Card Profile	V8.1	**Card Profile**	

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Facilities, Security and
Emergency Management

February 10, 2025

MEMORANDUM FOR Jennifer Duncan
Chief, Adjudications and Compliance
Personnel Security

FROM: Miranda Dillaman
Personnel Security Specialist
Facilities, Security & Emergency Management

Subject: Waiver of Pre-Appointment Background Investigation Requirements for Appointment to Special-Sensitive Positions

This is a request for a waiver of the pre-appointment background investigation requirements for Gregory Hogan's appointment to a special-sensitive position. This individual has been selected for the position of Chief Information Officer with the Office of the Chief Information Officer.

Executive Order 10450, "Security Requirements for Government Employment", Executive Order 12968, "Access to Classified Information", and Security Executive Agent Directive 8, (SEAD 8) provide that in exceptional circumstances or in an emergency, when official functions must be performed prior to the completion of the investigation and adjudication process or when in the national interest, an individual may be appointed on a temporary basis to a special-sensitive position prior to the investigation's completion. A delay in appointment would be harmful to national security and adversely impact the organization's mission.

Upon approval, the U.S. Office of Personnel Management's (OPM's) Personnel Security will initiate the above-named individual's personal security package for an expedited background investigation and pre-waiver checks, as appropriate. It is in the Agency's best interest to affect this appointment as soon as possible.

(Note: A waiver cannot be issued unless mandated portions of the current Tier 5 have been favorably reviewed.)

DECISION:
☒Approved ☐Not Approved ☐Let's Discuss

2/10/2025

X Jennifer Duncan

Branch Chief, OPM-FSEM-Personnel Security

Signed by: Office of Personnel Management

OPM U.S. Office of Personnel Management

This is to certify that

Gregory Hogan

has completed the course

CY 2024 Classified National Security Information Awareness and Insider Threat Training

March 9, 2025

Tierra F. Elsey

From: Personnel Security Group
To: Sylke, Kimberly D.
Cc: Lowe, Dana S.; Nickerson, Tiffany V.; Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Duncan, Jennifer
Subject: OPM-5 - CLEARED 01/14/2025
Date: Tuesday, January 14, 2025 12:25:00 PM
Attachments: image001.png

Please note that this cleared message is for a temporary appointment for less than 180 days.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) [redacted] | OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Dillaman, Miranda C.
To: Sylke, Kimberly D.
Cc: Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Pettit, John; Lowe, Dana S.; Nickerson, Tiffany V.
Subject: RE: New Hire Information for Incoming Senior Advisor to the Director for Technology & Delivery OPM-5
Date: Monday, January 13, 2025 2:23:00 PM
Attachments: image003.png
image001.png

Hi Kim!

OPM-5 will need fingerprints (which I have been notified he came in for fingerprinting today). You will receive a separate EOD message.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) [redacted] OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Sylke, Kimberly D. <[redacted]@opm.gov>
Sent: Monday, January 13, 2025 1:50 PM
To: Dillaman, Miranda C. <[redacted]@opm.gov>
Cc: Garcia, Carmen E. <[redacted]@opm.gov>; Beckman, Christopher J. <[redacted]@opm.gov>; Davis, Melinda M. <[redacted]@opm.gov>; Pettit, John <[redacted]@opm.gov>; Lowe, Dana S. <[redacted]@opm.gov>; Nickerson, Tiffany V. <[redacted]@opm.gov>
Subject: New Hire Information for Incoming Senior Advisor to the Director for Technology & Delivery OPM-5

Good Afternoon Miranda,

Requesting temporary clearance (less than 180 days) for OPM-5 , incoming Senior Advisor to the Director. Attached are the required documents for your review.

Please let me know if you need any additional information or have any questions.

V/R

Kim

Kim Sylke (pronouns: she/her)

SUPERVISORY HR SPECIALIST, EXECUTIVE RESOURCES

Office of the Chief Human Capital Officer | U.S. Office of Personnel Management

1900 E. St. NW | Washington DC 20415

Office: (202) [redacted]

Email: [redacted]@opm.gov

OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | X | YouTube

Weaver, Tyler R.

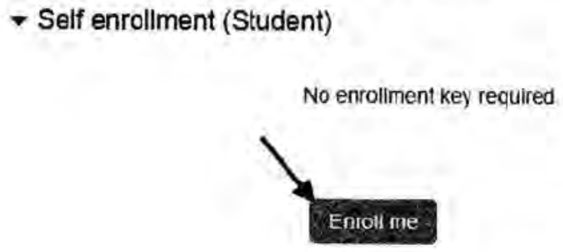
From:	Weaver, Tyler R.
Sent:	Wednesday, April 2, 2025 12:07 PM
To:	OPM-5
Cc:	Kennedy, Shellie L; Hicks, John A; Stugart, Sarah B.
Subject:	OPM-5 - Top Secret/SCI Clearance Request
Importance:	High

Good afternoon OPM-5,

As part of your duties with USOPM, it has been requested that you be granted access to Top Secret classified information. Additionally, it was further requested that you be processed for SCI access. The Top-Secret access is required to be granted prior to the SCI access and this email informs you of the requirements for the Top-Secret clearance access only. Once the Top-Secret clearance is in place you will be provided further instructions for the SCI access.

You are required to complete the on-line Classified National Security Awareness and Insider Threat Training located on the USOPM Learning Connection portal. The link to the training is: https://learningconnection.opm.gov/course/view.php?id=32655 Chrome Browser is recommended.

Access the OPM Learning Connection web site and locate the course. Directly below the course title will be an **Enroll Me** button that will allow you to self-enroll (see screen shot below). Once you click that button, you will receive an email stating that you are enrolled. You do not have to open the email or do anything with it. You should be able to click on the course's link to enter the training modules.



*If you do not see any of the above steps when you log on do a key word search for the course by typing or copying and pasting the following into the course search box: **CY 2024 Classified National Security Information Awareness and Insider Threat Training**. The course should now be displayed for you to choose.

You must complete the on-line training and pass it with a score of at least 80. After you complete the training, you must print your certificate. If you cannot obtain the certificate, please obtain a copy/snapshot of the actual test results. Send me a copy of your certificate/test results by email attachment to [redacted]@opm.gov. Upon receipt of the certificate, arrangements will be made to complete the SF 312, Classified Information Nondisclosure Agreement.

If you encounter any technical difficulties with the OPM Learning Connection, please refer to the website itself for instructions on how to contact the Help Desk.

If you have any questions regarding the clearance process, please let me know.

Thank you!

Tyler Weaver | Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
OPM.gov

OPM U.S. Office of Personnel Management

From: Personnel Security Group
To: Sylke, Kimberly D.
Cc: Lowe, Dana S.; Nickerson, Tiffany V.; Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Duncan, Jennifer; Hazlett, Amber L.; Mitchell, Diana
Subject: OPM-5 - CLEARED 02/18/2025
Date: Tuesday, February 18, 2025 12:46:00 PM
Attachments: image001.png

**Please note that this cleared message is for a permanent position over 180 days. The individual was previously cleared for less than 180 days.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) [redacted] | OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Dillaman, Miranda C.
To: Sylke, Kimberly D.
Cc: Davis, Melinda M.; Mitchell, Diana; Hazlett, Amber L.; Nickerson, Tiffany V.; Lowe, Dana S.; Dennis, Natasha
Subject: RE: OPM-5 (Schedule C) - Senior Advisor to the Director
Date: Thursday, January 30, 2025 7:24:00 AM
Attachments: image002.png

Hi Kim!

OPM-5 will need a full investigation on the 86. Fingerprints are not needed. I will take care of the eApp, email and cc you.

Thanks!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) [redacted] | OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Sylke, Kimberly D. <[redacted]@opm.gov>
Sent: Wednesday, January 29, 2025 4:28 PM
To: Dillaman, Miranda C. <[redacted]@opm.gov>
Cc: Davis, Melinda M. <[redacted]@opm.gov>; Mitchell, Diana <[redacted]@opm.gov>; Hazlett, Amber L. <[redacted]@opm.gov>; Nickerson, Tiffany V. <[redacted]@opm.gov>; Lowe, Dana S. <[redacted]@opm.gov>; Dennis, Natasha <[redacted]@opm.gov>
Subject: OPM-5 (Schedule C) - Senior Advisor to the Director

Hi Miranda,

Requesting clearance to move OPM-5 to a Senior Advisor to the Director (Schedule C) position permanently. Attached are following documents for your review:

- Resume
- PD
- New Hire Information

Please let me know if you need additional information.

V/R
Kim

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
INVESTIGATIONS SERVICE
WASHINGTON, DC 20415

CERTIFICATION OF INVESTIGATION

DATE: 03/18/2025

SUBMITTING OFFICE: SON - 133H SECURITY OFFICE: SOI - OM00

OPM
ATTN: CSEA
P.O. BOX 618
1137 BRANCHTON ROAD
BOYERS, PA 16018

NAME: OPM-5

SSN: [redacted] DOB: [redacted] POSITION: SENIOR ADVISOR TO TH

CASE TYPE: T5 CLOSING DATE: 03/18/2025 OPM CASE #: 2509900345
EXTRA COVERAGE: L / BVS
3 / ADVANCED REPORT OF NAC
PT / PRESIDENTIAL TRANSITION CASES
POSITION CODE : /

SCHEDULED DATE: 02/07/2025

INVESTIGATION CONDUCTED FROM: SF86 (7/17)

THIS CERTIFIES THAT A BACKGROUND INVESTIGATION ON THE PERSON IDENTIFIED ABOVE HAS BEEN COMPLETED. THE RESULTS OF THIS INVESTIGATION WERE SENT TO THE SECURITY OFFICE FOR A SECURITY/SUITABILITY DETERMINATION.

****

AGENCY CERTIFICATION: THE RESULTS OF THIS INVESTIGATION HAVE BEEN REVIEWED, AND A FINAL DETERMINATION HAS BEEN MADE.

AGENCY CERTIFYING OFFICIAL SARA ARBLASTER Digitally signed by SARA ARBLASTER Date: 2025.03.21 14:39:02 -04'00' DATE

FILE THIS CERTIFICATE ON THE PERMANENT SIDE OF THE PERSON'S OFFICIAL PERSONNEL FOLDER AFTER THE FINAL AGENCY DETERMINATION IS MADE.

Personnel Security Group

From: Personnel Security Group
Sent: Friday, March 21, 2025 2:54 PM
To: OPM-5
Subject: OPM-5 - NOTIFICATION OF COMPLETION OF INVESTIGATIVE PROCESS

Congratulations Mr. OPM-5,

The background investigation for your employment with the U.S. Office of Personnel Management was favorably adjudicated by Personnel Security on March 21, 2025. Your investigation was favorably adjudicated under both 5 CFR 731, Suitability Guidelines and E.O. 12968, National Security Adjudicative Guidelines. If your position requires access to classified information, you are eligible to be processed for a security clearance equivalent to your Position Designation. In order to complete the security clearance process, you will need to be nominated by your Division Director utilizing the OPM Form 1680 (Issuance of a Security Clearance) which can be requested from FSEM Personnel Security. If you have any questions regarding this notice or any other Personnel Security related matter, please contact me at the number below.

On October 1, 2019, as authorized by Executive Order 13869, the mission, records, and personnel of the OPM, National Background Investigations Bureau, transferred to the Department of Defense, Defense Counterintelligence and Security Agency (DCSA). Accordingly, as of October 1, 2019, in order to obtain a copy of your background investigation, request an amendment to your records, or file a FOIA request related to background investigation data or records, please follow the instructions at DCSA's website: https://www.dcsa.mil/mc/pv/mbi/mr/. If you have specific questions, you may contact the DCSA Freedom of Information and Privacy Office for Investigations at: (878)[redacted].

Thank you,

Sara Arblaster
Personnel Security Specialist
U.S. Office of Personnel Management
Facilities, Security & Emergency Management-Personnel Security
o: (202)[redacted]
f: (724)[redacted]
[redacted]@opm.gov
OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Facilities, Security and Emergency Management

February 18, 2025

MEMORANDUM FOR Jennifer Duncan
Chief, Adjudications and Compliance
Personnel Security

FROM: Miranda Dillaman
Personnel Security Specialist
Facilities, Security & Emergency Management

Subject: Waiver of Pre-Appointment Background Investigation Requirements for Appointment to Critical-Sensitive Positions

This is a request for a waiver of the pre-appointment background investigation requirements for OPM-5 OPM-5's appointment to a critical-sensitive position. This individual has been selected for the position of Senior Advisor to the Director of Information Technology with the Office of the Director.

Executive Order 10450, "Security Requirements for Government Employment", Executive Order 12968, "Access to Classified Information", and Security Executive Agent Directive 8, (SEAD 8) provide that in exceptional circumstances or in an emergency, when official functions must be performed prior to the completion of the investigation and adjudication process or when in the national interest, an individual may be appointed on a temporary basis to a critical-sensitive position prior to the investigation's completion. A delay in appointment would be harmful to national security and adversely impact the organization's mission.

Upon approval, the U.S. Office of Personnel Management's (OPM's) Personnel Security will initiate the above-named individual's personal security package for an expedited background investigation and pre-waiver checks, as appropriate. It is in the Agency's best interest to affect this appointment as soon as possible.

(Note: A waiver cannot be issued unless mandated portions of the current Tier 5 have been favorably reviewed.)

DECISION:
[✓ Approved] ☐Not Approved ☐Let's Discuss

X [illegible]
Branch Chief, OPM-FSEM-Personnel Security

From: Personnel Security Group
To: Sylke, Kimberly D.
Cc: Lowe, Dana S.; Nickerson, Tiffany V.; Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Duncan, Jennifer
Subject: OPM-6 - CLEARED 01/24/2025
Date: Friday, January 24, 2025 10:46:00 AM
Attachments: image001.png

Please note that this cleared message is for a temporary appointment for less than 180 days.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) [redacted] | OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Davis, Melinda M.
To: Beckman, Christopher J.
Cc: Dillaman, Miranda C.
Subject: FW: Rush on Onboarding
Date: Friday, January 24, 2025 7:55:51 AM
Attachments: Outlook-m20yup3t.png
image003.png

Chris-
We have no record fingerprints but we do not have the 306 or release. Kim is supposed to be reaching out this morning to obtain these. That is the latest status we have. As soon as we get the paperwork we can clear. Thanks.

Mindy Davis | Division Director-Personnel Security

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management
M: (202) [redacted] | OPM.gov
T: (202) [redacted]

Follow us on LinkedIn | Twitter | YouTube

From: Hilliard, Everette <[redacted]@opm.gov>
Sent: Friday, January 24, 2025 5:54 AM
To: Davis, Melinda M. <[redacted]@opm.gov>; Dillaman, Miranda C. <[redacted]@opm.gov>; Beckman, Christopher J. <[redacted]@opm.gov>
Subject: Fwd: Rush on Onboarding

Sent from my iPhone

Begin forwarded message:

> **From:** "Garcia, Carmen E." <[redacted]@opm.gov>
> **Date:** January 23, 2025 at 10:07:38 PM EST
> **To:** "Ezell, Charles E." <[redacted]@opm.gov>, "Hilliard, Everette" <[redacted]@opm.gov>
> **Cc:** OPM-7 @opm.gov>
> **Subject: Re: Rush on Onboarding**
>
> Good Evening Acting Director,
>
> I will prioritize this and make sure we see this through expeditiously. We just need to execute an MOU and it's drafted and signed on our end. I just need to get in touch with their respective agencies for their signature in order to finalize the detail.

We hope to have resolution early tomorrow.

Thank you,
Carmen

Get Outlook for iOS

From: Ezell, Charles E. <[redacted]@opm.gov>
Sent: Thursday, January 23, 2025 10:04:32 PM
To: Garcia, Carmen E. <[redacted]@opm.gov>; Hilliard, Everette <[redacted]@opm.gov>
Cc: OPM-7 @opm.gov>
Subject: Rush on Onboarding

Reid & Carmen, we need to quickly onboard the two DOGE employees tomorrow if at all possible. I'm not sure where they are in the process but we are desperately needing their engineering skills to help with a special project for President Trump.

- OPM-4
- OPM-6

.ce

Chuck Ezell

Acting Director

U.S. Office of Personnel Management

(478) [redacted]

[redacted]@opm.gov

OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Personnel Security Group
To: Sylke, Kimberly D.
Cc: Lowe, Dana S.; Nickerson, Tiffany V.; Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Duncan, Jennifer
Subject: OPM-8 - CLEARED 01/14/2025
Date: Tuesday, January 14, 2025 6:05:00 PM
Attachments: image001.png

Please note that this cleared message is for a temporary appointment for less than 180 days.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) [redacted] | OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Dillaman, Miranda C.
To: Sylke, Kimberly D.
Cc: Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Lowe, Dana S.
Subject: RE: New Hire Information for Incoming Senior Advisor to the Director (OPM-8)
Date: Tuesday, January 14, 2025 3:42:00 PM
Attachments: image004.png
image005.png
image001.png

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) [redacted] | OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Sylke, Kimberly D. <[redacted]@opm.gov>
Sent: Tuesday, January 14, 2025 3:30 PM
To: Dillaman, Miranda C. <[redacted]@opm.gov>
Cc: Garcia, Carmen E. <[redacted]@opm.gov>; Beckman, Christopher J. <[redacted]@opm.gov>; Davis, Melinda M. <[redacted]@opm.gov>; Lowe, Dana S. <[redacted]@opm.gov>
Subject: Re: New Hire Information for Incoming Senior Advisor to the Director (OPM-8)

Hi Miranda, updated 306 attached.

V/R
Kim

From: Dillaman, Miranda C. <[redacted]@opm.gov>
Sent: Monday, January 13, 2025 2:40 PM
To: Sylke, Kimberly D. <[redacted]@opm.gov>
Cc: Garcia, Carmen E. <[redacted]@opm.gov>; Beckman, Christopher J. <[redacted]@opm.gov>; Davis, Melinda M. <[redacted]@opm.gov>; Pettit, John <[redacted]@opm.gov>; Lowe, Dana S. <[redacted]@opm.gov>; Nickerson, Tiffany V. <[redacted]@opm.gov>
Subject: RE: New Hire Information for Incoming Senior Advisor to the Director (OPM-8)

Hi Kim!

OPM-8 will need fingerprints (which I have been notified OPM-8 came in for fingerprinting today). Would you mind having OPM-8 submit a new 306? The answers to the questions aren't populating and the date signed isn't correct.

You will receive a separate EOD message.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) [redacted] | OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Sylke, Kimberly D. <[redacted]@opm.gov>
Sent: Monday, January 13, 2025 2:13 PM
To: Dillaman, Miranda C. <[redacted]@opm.gov>
Cc: Garcia, Carmen E. <[redacted]@opm.gov>; Beckman, Christopher J. <[redacted]@opm.gov>; Davis, Melinda M. <[redacted]@opm.gov>; Pettit, John <[redacted]@opm.gov>; Lowe, Dana S. <[redacted]@opm.gov>; Nickerson, Tiffany V. <[redacted]@opm.gov>
Subject: New Hire Information for Incoming Senior Advisor to the Director (OPM-8)

Good Afternoon Miranda,

Requesting temporary clearance (less than 180 days) for OPM-8 , incoming Senior Advisor to the Director. Attached are the required documents for your review.

Please let me know if you need any additional information or have any questions.

V/R

Kim

Kim Sylke (pronouns: she/her)

SUPERVISORY HR SPECIALIST, EXECUTIVE RESOURCES

Office of the Chief Human Capital Officer | U.S. Office of Personnel Management

1900 E. St. NW | Washington DC 20415

Office: (202) [redacted]

Email: [redacted]@opm.gov

OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | X | YouTube

Stugart, Sarah B.

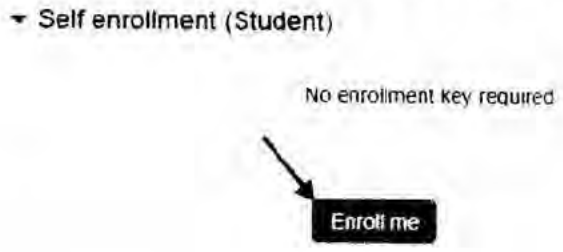
From:	Stugart, Sarah B.
Sent:	Tuesday, March 4, 2025 1:54 PM
To:	OPM-8
Subject:	Clearance- OPM-8
Importance:	High

Good afternoon, OPM-8 .

As part of your duties with USOPM, it has been requested that you be granted access to Top Secret classified information. Additionally, it was further requested that you be processed for SCI access. The Top-Secret access is required to be granted prior to the SCI access and this email informs you of the requirements for the Top-Secret clearance access only. Once the Top-Secret clearance is in place you will be provided further instructions for the SCI access.

You are required to complete the on-line Classified National Security Awareness and Insider Threat Training located on the USOPM Learning Connection portal. The link to the training is: https://learningconnection.opm.gov/course/view.php?id=32655 Chrome Browser is recommended.

Access the OPM Learning Connection web site and locate the course. Directly below the course title will be an **Enroll Me** button that will allow you to self-enroll (see screen shot below). Once you click that button, you will receive an email stating that you are enrolled. You do not have to open the email or do anything with it. You should be able to click on the course's link to enter the training modules.



*If you do not see any of the above steps when you log on do a key word search for the course by typing or copying and pasting the following into the course search box: **CY 2024 Classified National Security Information Awareness and Insider Threat Training.** The course should now be displayed for you to choose.
You must complete the on-line training and pass it with a score of at least 80. After you complete the training, you must print your certificate. If you cannot obtain the certificate, please obtain a copy/snapshot of the actual test results. Send me a copy of your certificate/test results by email attachment to [redacted]@opm.gov. Upon receipt of the certificate, arrangements will be made to complete the SF 312, Classified Information Nondisclosure Agreement.

If you encounter any technical difficulties with the OPM Learning Connection, please refer to the website itself for instructions on how to contact the Help Desk.

If you have any questions regarding the clearance process, please let me know. Thank you.

Thank you.

Sarah Stugart | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
Phone: 202[redacted] | OPM.gov
OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

Personnel Security Group

From: Personnel Security Group
Sent: Tuesday, March 4, 2025 11:26 AM
To: OPM-8
Subject: OPM-8 - NOTIFICATION OF COMPLETION OF INVESTIGATIVE PROCESS

Congratulations OPM-8 ,

The background investigation for your employment with the U.S. Office of Personnel Management was favorably adjudicated by Personnel Security on March 4, 2025. Your investigation was favorably adjudicated under both 5 CFR 731, Suitability Guidelines and E.O. 12968, National Security Adjudicative Guidelines. If your position requires access to classified information, you are eligible to be processed for a security clearance equivalent to your Position Designation. In order to complete the security clearance process, the OPM Form 1680 (Issuance of a Security Clearance) has been submitted and you will be contacted separately by a member of the Personnel Security Staff to complete a security clearance briefing/training and to execute the SF 312 Non-disclosure Agreement prior to being granted access to classified information. If you have any questions regarding this notice or any other Personnel Security related matter, please contact me at the number below.

On October 1, 2019, as authorized by Executive Order 13869, the mission, records, and personnel of the OPM, National Background Investigations Bureau, transferred to the Department of Defense, Defense Counterintelligence and Security Agency (DCSA). Accordingly, as of October 1, 2019, in order to obtain a copy of your background investigation, request an amendment to your records, or file a FOIA request related to background investigation data or records, please follow the instructions at DCSA's website: https://www.dcsa.mil/mc/pv/mbi/mr/. If you have specific questions, you may contact the DCSA Freedom of Information and Privacy Office for Investigations at: (878)[redacted]

Thank you,

Sara Arblaster
Personnel Security Specialist
U.S. Office of Personnel Management
Facilities, Security & Emergency Management-Personnel Security
o: (202)[redacted]
f: (724)[redacted]
[redacted]@opm.gov
OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Personnel Security Group
To: Sylke, Kimberly D.
Cc: Lowe, Dana S.; Nickerson, Tiffany V.; Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Duncan, Jennifer; Hazlett, Amber L.; Mitchell, Diana
Subject: OPM-8 - CLEARED 02/12/2025
Date: Wednesday, February 12, 2025 1:46:00 PM
Attachments: image001.png

**Please note that this cleared message is for a permanent position over 180 days. The individual was previously cleared for less than 180 days.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) [redacted] | OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Dillaman, Miranda C.
To: Sylke, Kimberly D.
Cc: Davis, Melinda M.; Mitchell, Diana; Hazlett, Amber L.; Nickerson, Tiffany V.; Lowe, Dana S.; Dennis, Natasha
Subject: RE: OPM-8 (Schedule C) - Senior Advisor
Date: Thursday, January 30, 2025 5:03:00 PM
Attachments: image002.png

Hi Kim!

OPM-8 will need a full investigation on the 86. Fingerprints are not needed. I will take care of the eApp, email and cc you.

Thanks!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) [redacted] | OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Sylke, Kimberly D. <[redacted]@opm.gov>
Sent: Thursday, January 30, 2025 10:22 AM
To: Dillaman, Miranda C. <[redacted]@opm.gov>
Cc: Davis, Melinda M. <[redacted]@opm.gov>; Mitchell, Diana <[redacted]@opm.gov>; Hazlett, Amber L. <[redacted]@opm.gov>; Nickerson, Tiffany V. <[redacted]@opm.gov>; Lowe, Dana S. <[redacted]@opm.gov>; Dennis, Natasha <[redacted]@opm.gov>
Subject: OPM-8 (Schedule C) - Senior Advisor

Good Morning Miranda,

Requesting clearance to move OPM-8 to a Senior Advisor (Schedule C) position permanently. Attached are following documents for your review:

- Resume
- PD *(This is a new PD, so it doesn't have a position designation record yet.)*
- New Hire Information

Please let me know if you need additional information.

V/R
Kim

GSA USACCESS Program

Applicant Status Report **Report Print Date :** **04/14/2025** **12:47:51PM**

APPLICANT INFORMATION - Page 2

Enrollment ID [redacted] **Name** OPM-8 **DOB** [redacted]

ADJUDICATION INFORMATION

Adjudication Status	ADJUDICATED		
Adjudication Create Date / Last Update	12-Feb-2025 13:50 / 04-Mar-2025 11:40		
NCHC/FBI	APPROVED	**NCHC/FBI Adjudicator ID**	[redacted]
NACI	APPROVED	**NACI Adjudicator ID**	[redacted]
Adj Last Update Agency	OFFICE OF PERSONNEL MANAGEMENT		
Adj Last Update Agency Date	04-Mar-2025 11:40		
PIV Agency Specific Criteria Status		**PIV-I Agency Specific Criteria Status**	
PIV Agency Specific Criteria Date		**PIV-I Agency Specific Criteria Date**	

ENROLLMENT INFORMATION

Enrollment Status	COMPLETE	**Last Enrollment Date**	14-Feb-2025 9:43
Enrollment Create Date	12-Feb-2025 13:50	**Enrollment Last Update**	14-Feb-2025 9:43
Document Referral	NO		
Enrollment Site ID/Description	102415 / OPM LCS 10		
Enrollment Site Address: Line 1	1H17		
Line 2	1900 E ST NW		
Line 3			
City /State / Zip Code	WASHINGTON / DC / 20415		

ISSUANCE INFORMATION

CURRENT CARD		REPLACEMENT CARD	
Issuance Status	ACTIVE	**Issuance Status**	NO STATUS
Create/Last Update Date	12-Feb-2025 13:50 / 25-Feb-2025 16:26	**Create/Last Update Date**	/
CMS Card ID	[redacted]	**CMS Card ID**	
Card ID	1 **Card Destroyed** NO	**Card ID**	
FASC-N	[redacted]	**FASC-N**	
Card UUID	[redacted]	**Card UUID**	
Issuance Sub-Status	ACTIVATED	**Issuance Sub-Status**	NO STATUS
Issuance Cred Option	PIV	**Issuance Cred Option**	
Certificate Set	4	**Certificate Set**	
Card Profile	V8.1	**Card Profile**	

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
INVESTIGATIONS SERVICE
WASHINGTON, DC 20415

CERTIFICATION OF INVESTIGATION

DATE: 03/03/2025

SUBMITTING OFFICE: SON - 133H SECURITY OFFICE: SOI - OM00

OPM
ATTN: CSEA
P.O. BOX 618
1137 BRANCHTON ROAD
BOYERS, PA 16018

NAME: OPM-8

SSN: [redacted] DOB [redacted] POSITION: SENIOR ADVISOR - PRE

CASE TYPE: T5 CLOSING DATE: 03/03/2025 OPM CASE #: 2509900384
EXTRA COVERAGE: L / BVS
3 / ADVANCED REPORT OF NAC
PT / PRESIDENTIAL TRANSITION CASES
POSITION CODE : /

SCHEDULED DATE: 02/11/2025

INVESTIGATION CONDUCTED FROM: SF86 (7/17)

THIS CERTIFIES THAT A BACKGROUND INVESTIGATION ON THE PERSON IDENTIFIED ABOVE HAS BEEN COMPLETED. THE RESULTS OF THIS INVESTIGATION WERE SENT TO THE SECURITY OFFICE FOR A SECURITY/SUITABILITY DETERMINATION.

****

AGENCY CERTIFICATION: THE RESULTS OF THIS INVESTIGATION HAVE BEEN REVIEWED, AND A FINAL DETERMINATION HAS BEEN MADE.

AGENCY CERTIFYING OFFICIAL SARA ARBLASTER Digitally signed by SARA ARBLASTER Date: 2025.03.04 10:44:24 -05'00' DATE

FILE THIS CERTIFICATE ON THE PERMANENT SIDE OF THE PERSON'S OFFICIAL PERSONNEL FOLDER AFTER THE FINAL AGENCY DETERMINATION IS MADE.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Facilities, Security and
Emergency Management

February 12, 2025

MEMORANDUM FOR Jennifer Duncan
Chief, Adjudications and Compliance
Personnel Security

FROM: Miranda Dillaman
Personnel Security Specialist
Facilities, Security & Emergency Management

Subject: Waiver of Pre-Appointment Background Investigation Requirements for Appointment to Critical-Sensitive Positions

This is a request for a waiver of the pre-appointment background investigation requirements for OPM-8 OPM-8 's appointment to a critical-sensitive position. This individual has been selected for the position of Senior Advisor with the Office of the Director.

Executive Order 10450, "Security Requirements for Government Employment", Executive Order 12968, "Access to Classified Information", and Security Executive Agent Directive 8, (SEAD 8) provide that in exceptional circumstances or in an emergency, when official functions must be performed prior to the completion of the investigation and adjudication process or when in the national interest, an individual may be appointed on a temporary basis to a critical-sensitive position prior to the investigation's completion. A delay in appointment would be harmful to national security and adversely impact the organization's mission.

Upon approval, the U.S. Office of Personnel Management's (OPM's) Personnel Security will initiate the above-named individual's personal security package for an expedited background investigation and pre-waiver checks, as appropriate. It is in the Agency's best interest to affect this appointment as soon as possible.

(Note: A waiver cannot be issued unless mandated portions of the current Tier 5 have been favorably reviewed.)

DECISION:
☒ Approved ☐ Not Approved ☐ Let's Discuss

Recoverable Signature

X Jennifer Duncan
Branch Chief, OPM-FSEM-Personnel Security

Signed by: Office of Personnel Management

OPM U.S. Office of Personnel Management

This is to certify that

OPM-8

has completed the course

CY 2024 Classified National Security Information Awareness and Insider Threat Training

March 8, 2025

Tierra F. Elsey